DOCUMENT RESUME

ED 463 762 IR 058 438

AUTHOR	Plum, Terry, Comp.; Bleiler, Richard, Comp.
TITLE	User Authentication. SPEC Kit.
INSTITUTION	Association of Research Libraries, Washington, DC. Office of Leadership and Management Services.
ISSN	ISSN-0160-3582
PUB DATE	2001-12-00
NOTE	103p.; Each SPEC Kit contains an executive summary of the survey results (previously printed as the SPEC Flyer). Published six times per year.
AVAILABLE FROM	ARL Publications Distribution Center, P.O. Box 531, Annapolis Junction, MD 20701-0531 ($35, ARL member; $45, nonmembers; plus $6 shipping and handling). Tel: 301-362-8196; Fax: 301-206-9789; e-mail: pubs@arl.org; Web site: http://www.arl.org/pubscat/index.html.
PUB TYPE	Collected Works - Serials (022) -- Reports - Research (143) -- Tests/Questionnaires (160)
JOURNAL CIT	SPEC Kit; n267 Dec 2001
EDRS PRICE	MF01/PC05 Plus Postage.
DESCRIPTORS	*Academic Libraries; Computer Uses in Education; Electronic Libraries; Foreign Countries; Higher Education; Library Associations; *Library Services; Library Surveys; Online Systems; Questionnaires; *Research Libraries; *Users (Information); World Wide Web
IDENTIFIERS	Association of Research Libraries; Authenticity; Canada; *Electronic Resources; United States

ABSTRACT

This SPEC (Systems and Procedures Exchange Center) Kit presents the results of a survey of Association of Research Libraries (ARL) member libraries designed to examine the systems research libraries use to authenticate and authorize the users of their online networked information resources. A total of 52 of 121 ARL member libraries responded to the survey. A copy of the questionnaire with tabulated results is presented. Representative documents include: explanations for users from the University of Alberta, University of California-Davis, University of California-Irvine, University of Colorado, Colorado State University, University of Connecticut, Cornell University (New York), Dartmouth College (New Hampshire), Duke University (North Carolina), University of Florida, McMaster University (Ontario), University of Manitoba, Massachusetts Institute of Technology, University of North Carolina, University of Oregon, University of Washington, Washington University (Missouri), and University of Waterloo (Ontario); technical specifications from Cornell University, Universite Laval (Quebec); and project plans from the University of Connecticut and University of Waterloo. (Contains 43 references.) (MES)

Reproductions supplied by EDRS are the best that can be made
from the original document.

ED 463 762

SPEC Kit 267

User Authentication
December 2001

PERMISSION TO REPRODUCE AND DISSEMINATE THIS MATERIAL HAS BEEN GRANTED BY

C. A. Mandel

TO THE EDUCATIONAL RESOURCES INFORMATION CENTER (ERIC)

1

U.S. DEPARTMENT OF EDUCATION
Office of Educational Research and Improvement
EDUCATIONAL RESOURCES INFORMATION CENTER (ERIC)

N This document has been reproduced as received from the person or organization originating it.

☐ Minor changes have been made to improve reproduction quality.

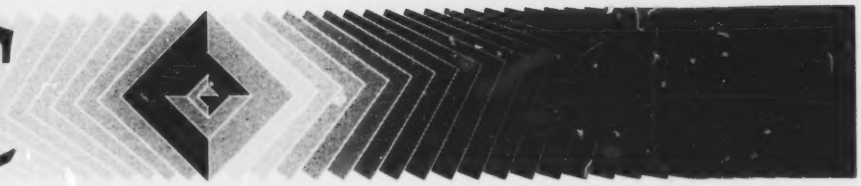
• Points of view or opinions stated in this document do not necessarily represent official OERI position or policy.

IR058438

Association of Research Libraries
Office of Leadership and Management Services

BEST COPY AVAILABLE

SPEC



User Authentication

A SPEC Kit compiled by

Terry Plum
Assistant Professor
Simmons Graduate School of Library and Information Science

Richard Bleiler
Humanities Reference Librarian
University of Connecticut

December 2001

Series Editor: Lee Anne George

SPEC Kits are published by the

Association of Research Libraries
Office of Leadership and Management Services
21 Dupont Circle, NW, Suite 800
Washington, D.C. 20036-1118
(202) 296-2296 Fax (202) 872-0884
<http://www.arl.org/olms/infosvcs.html>
<pubs@arl.org>

ISSN 0160 3582

Copyright © 2001
The papers in this compilation are copyrighted by the Association of Research Libraries. ARL grants blanket permission to reproduce and distribute copies of these works for nonprofit, educational, or library purposes, provided that copies are distributed at or below cost, and that ARL, the source, and copyright notice are included on each copy. This permission is in addition to rights of reproduction granted under Sections 107, 108, and other provisions of the U.S. Copyright Act.

The paper used in this publication meets the requirements of ANSI/NISO Z39.48-1992 (Permanence of Paper).

SPEC

Supporting Effective Library Management for Over Twenty Years

Committed to assisting research and academic libraries in the continuous improvement of management systems, OLMS has worked since 1970 to gather and disseminate the best practices for library needs. As part of its committment, OLMS maintains an active publications program best known for its SPEC Kits. Through the OLMS Collaborative Research/Writing Program, librarians work with ARL staff to design SPEC surveys and write publications. Originally established as an information source for ARL member libraries, the SPEC series has grown to serve the needs of the library community worldwide.

What Are SPEC Kits?

Published six times per year, SPEC Kits contain the most valuable, up-to-date information on the latest issues of concern to libraries and librarians today. They are the result of a systematic survey of ARL member libraries on a particular topic related to current practice in the field. Each SPEC Kit contains an executive summary of the survey results (previously printed as the SPEC Flyer); survey questions with tallies and selected comments; the best representative documents from survey participants, such as policies, procedures, handbooks, guidelines, websites, records, brochures, and statements; and a selected reading list—both in print and online sources—containing the most current literature available on the topic for further study.

Subscribe to SPEC

Subscribers tell us that the information contained in SPEC Kits is valuable to a variety of users, both inside and outside the library. SPEC purchasers use the documentation found in SPEC Kits as a point of departure for research and problem solving because they lend immediate authority to proposals and set standards for designing programs or writing procedure statements. SPEC Kits also function as an important reference tool for library administrators, staff, students, and professionals in allied disciplines who may not have access to this kind of information.

SPEC Kits can be ordered directly from the ARL Publications Distribution Center. To order, call (301) 362-8196, fax (301) 206-9789, email <pubs@arl.org>, or go to <http://www.arl.org/pubscat/index.html>.

Information on SPEC and other OLMS products and services can be found on the ARL website at <http://www.arl.org/olms/infosvcs.html>. The website for SPEC is <http://www.arl.org/spec/index.html>. The executive summary or flyer for each kit after December 1993 can be accessed free of charge at the SPEC website.

SPEC Kit 267

User Authentication
December 2001

Survey

EXECUTIVE SUMMARY 9
SURVEY RESULTS 14
RESPONDING INSTITUTIONS 22

Representative Documents

EXPLANATIONS FOR USERS

University of Alberta

Off Campus Access to Electronic Library Resources 26

University of California–Davis

Access to UC Davis Licensed Resources 27

University of California–Irvine

Connecting from Home: Remote Access Guide 29

University of Colorado

Remote Access to Chinook: CU–Boulder Students, Staff, and Faculty 31

Colorado State University

Remote Access to Library Databases: Proxy Server Instructions 33

How the Proxy Server Works 34

Without the Proxy Server 35

With the Proxy Server 36

University of Connecticut

Obtaining an Account on the University of Connecticut Proxy Server 37

Cornell University

Proxy Server for Access to Library Resources from Outside Cornell 39

Dartmouth College
Kerberos Authentication at Dartmouth 41
Kerberos Authentication. How it Works 42
Duke University
Remote Access Options. Connecting from Off-campus 43
University of Florida
Guide to Remote Access to Library Databases 44
Guide to Remote Access Using a Proxy Connection 46
McMaster University
Off Campus Access: A Guide to the McMaster Proxy Service 48
University of Manitoba
Using the Proxy Server to Access Restricted Databases and Web Resources 49
Massachusetts Institute of Technology
Obtaining MIT Certificates: Quick Guide 51
University of North Carolina
Off-campus Access via Proxy Server 52
University of Oregon
Off-campus Access to Library Databases 55
University of Washington
About UW NetIDs 56
Connecting to the Libraries 57
Washington University
Proxy Setup Instructions 59
University of Waterloo
Connect from Home 61

TECHNICAL SPECIFICATIONS
Cornell University
How the Proxy Web Server Works 64
Université Laval
Serveur Mandataire. Version 1.0. Détails Techniques 66

PROJECT PLANS

University of Connecticut

University ITS. Authentication Project 84

Authentication Project Profile 85

University of Waterloo

Identification, Authentication, and Electronic Commerce 94

Final Report for the ID-AUTH-ECOMM Prototype. Preface 95

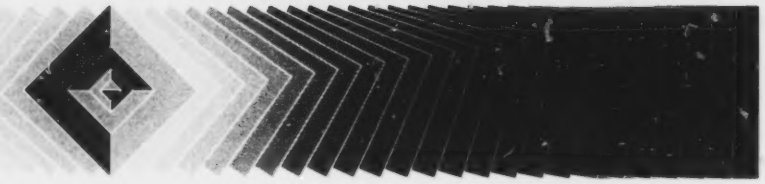
Final Report. Introduction 96

Final Report. Recommendations 98

Selected Resources

BOOKS AND JOURNAL ARTICLES 101

SPEC



SURVEY

Executive Summary

Introduction

Until the advent of the World Wide Web and the concomitant development of global computer networks, most research libraries could provide access to their resources with few concerns about the status of those who sought the information, or concerns that the information was restricted to certain classes of users. Developments in computer technologies have irrevocably altered library operations, and it is now the exceptional library that has not in some way responded to the challenges of authenticating and authorizing its users, particularly those users needing to access the library's systems and networked information resources from remote locations. Furthermore, licenses for networked information resources increasingly require authentication controls and need to specify different levels of authorization.

Authentication and authorization are complex access management processes that involve the verification of the identity and status of the user, the ways in which IP ranges are limited, the processes by which information technology support is handled, and the systems by which authentication information and authorization are maintained.

This SPEC survey is designed to examine the systems that research libraries use to authenticate and authorize the users of their online networked information resources. For the purposes of this survey, authentication is defined as the process of determining whether someone or something is, in fact, who or what he declares himself to be. Authorization is the process of giving someone permission to do or have something, including privileges of use, such as access to file directories, amount of allocated storage space, access to licensed electronic resources, and so forth. Networked information resources are defined as electronically accessible information resources (e.g., library or academically developed databases, university databases, commercial databases, full-text services, e-journals, etc.) funded or enabled by the library, which are made available to authorized users through an intentional and systematic network (LAN, WAN, dial-in, etc.).

This survey was distributed to the 121 ARL member libraries in spring 2001. Fifty-two libraries (43%) responded to the survey.

Authentication

Fifty-one of the responding institutions (98%) stated that they authenticated their users in some way. The one library reporting no authentication apparently limits by IP, has a proxy server, and offers remote access services to library resources through a modem pool. Therefore, all of the responding libraries authenticate users of networked resources.

In selecting user categories for authentication, 48 respondents (96%) authenticate staff, and 46 (92%) authenticate their undergraduate students, graduate students, and faculty. Seven libraries (14%) authenticate alumni and local community members, although their access to the library's networked electronic resources is apparently much reduced. Fourteen respondents (28%) report that they authenticate other categories, providing access to groups such as Friends of the Library, extension faculty and students, selected department-sponsored guest accounts, university affiliates, affiliated institutions, and external clients, including international clients.

There were 49 responses (96%) to the question about the number of networked information resources made available to authenticated users, but the numbers varied enormously, from 1 to 23,806. That these numbers are so disparate almost certainly

demonstrates that there is no agreement on the unit of analysis for measuring "networked information resources." A simple example will suffice in showing the nature of the problem: does JSTOR count as a single networked information resource, or is it the sum of its subscription modules, or is it the sum of the journal contents? And, if the latter, how are title changes treated? This problem is only exacerbated when one considers the number and variety of networked electronic resources potentially available to ARL member libraries.

Access Management Systems

There was equal divagation in the responses on the type of access management system used to authenticate users of networked information resources, although in this case the disparity appears to be the result of respondents using multiple systems. For example, 42 of the 51 responding libraries (82%) report using IP addresses to authenticate users of at least some portion of their networked electronic resources, while an overlapping 40 (78%) report the use of password and user ID. There is similar overlap among and within the other types of systems. (See question 4 in the Survey Results section for a chart of the types of systems used.)

Surprisingly few libraries (10, or 20%) use the ILS to authenticate patrons, and only four (8%) use a non-ILS gateway, such as OCLC's WebZ. Based on a review of the literature and websites, the number of libraries that use Public Key Infrastructure (PKI) is also unexpectedly small. Since only three libraries (6%) claim that they have enabled this scheme to authenticate patrons, perhaps PKI is as yet more discussed than implemented.

All together, 46 respondents report using some kind of proxy server. These libraries apparently are migrating from mechanical proxy systems (pac files) to application-level proxy servers or rewriters (such as EZproxy). Twenty-six libraries report using a mechanical proxy system, whereas 12 use an application-level rewriter. Two libraries use both. Fifteen respondents (33%) use EZproxy as the proxy server software, almost twice as many as use Apache (9 respondents or 20%), Squid (8, or 17%), or Web Access Management (III) (6, or 13%). Only three respondents use Netscape Iplanet Proxy, and one uses Microsoft Proxy. A small number of institutions are using homegrown or custom solutions. Of the 42 libraries that rely upon IP authentication, only four have neither a proxy server nor a modem pool, while only two still rely upon a dial-in modem pool exclusively for off-campus access.

Survey respondents were asked which database of patron information is used to verify eligible users. Again, it is evident that multiple systems are in use at many institutions. In the majority of instances (28 responses or 55%) some portion of the authentication system checks against a dynamic patron load or circulation patron record database with the ILS. Fewer institutions (20, or 39%) have a system that checks against a dynamic institutional personnel database. An equal number (14, or 28%) use a system check against a flat file extracted from the ILS or a system check against a separately created database of eligible users. Only seven (14%) use a system check against a flat file extracted from the institutional personnel database. Five respondents (10%) use other solutions, including a Virtual Personal Network and personal certificates.

Authorization

What services are being authorized after authentication? The access provided by credential-based (passwords, certificates, etc.) systems is widely distributed. At 35 institutions (69%), authenticated users can access their personal circulation record, while at 33 (65%) users can request interlibrary loans and document delivery and use e-mail. Other accessible services include holds and recalls on books (31 institutions or 61%), course registration information (29, or 57%), databases (28, or 55%), and both course reserve materials and file space on the network server (25, or 49%). Numbers were lower for accessing financial records and computer labs (21, or 41%) and lower still for accessing e-books and e-journals (20, or 39%). The figures continued to drop for accessing the library OPAC (19, or 37%), distance education courses (18, or 35%), and transcripts (17, or 33%). Only seven institutions (14%) use credential-based systems to provide access

to photocopy machines, dining facilities, and groupware.

The distribution of services provided by proxy systems and IP filtering is almost identical. The majority of institutions that use a proxy server provide access to databases (41, or 80%), e-journals (40, or 78%), and e-books (36, or 71%). Fourteen (27%) provide access to course reserve materials, and 11 (22%) to the library OPAC. There are few uses of the proxy server for other purposes, although six respondents (12%) report using it for distance education courses.

User Privacy

Questions of confidentiality and privacy policy are important to any web-based authentication system. Although this survey did not specifically inquire about privacy policies, it surveyed respondents about how user information is tied to the respective search session and whether such information is archived. Thirty-two of 49 respondents (65%) provide *anonymous access*, in which each session is anonymous and repeat users cannot be identified. Twenty-four (49%) provide *identified access*, in which actual identities are associated only with sessions, and 12 (25%) provide *pseudonymous access*, in which repeat users can be identified, but the identity of a specific user cannot be determined. These responses appear to be closely allied with the American Library Association (ALA) *Policy Concerning Confidentiality of Personally Identifiable Information about Library Users*. This policy states in part that, "Confidentiality extends to 'information sought or received, and materials consulted, borrowed or acquired,' and includes database search records, reference interviews, circulation records, interlibrary loan records, and other personally identifiable uses of library materials, facilities, or services." Nevertheless, ten respondents (20%) archive identified access data and eight (16%) provide pseudonymous access with demographic information that does not provide actual identities. The ALA *Policy on Confidentiality of Library Records* strongly recommends that, "Responsible officers of each library, cooperative system, and consortium in the United States formally adopt a policy which specifically recognizes its circulation records and other records identifying the name of library users to be confidential in nature." It appears that most libraries address this issue by refusing to store ID information with session data.

System Management

Who does the work of building and maintaining the authentication system? In general, much of the work is done within the library. Central library information technology (IT) staff manage the authentication and authorization systems in 46 of the responding institutions (90%). Institution or campus-wide IT staff manage them for 37 (73%) of the respondents and the vendor of the networked information resource manages authentication for 25 (49%). One respondent wrote that campus IT handles e-mail, registration, and distance education; the vendor handles IP authentication for e-journals, e-books, and online databases; and the library handles the other resources. This is a very traditional arrangement.

Question 9 asked how many IP-filtered resources are managed at the vendor, consortium, institution, or other level. The data again illustrate the difficulty of counting networked information resources with responses ranging from zero to more than 10,000. A general impression is that the vendor most often handles IP-based access restrictions to library resources.

At the 26 institutions that manage access by an ILS capable of accessing databases through Z39.50 (z-client), survey results indicate a fairly equal distribution across ILS vendors. Endeavor and III are each used by five of the 26 respondents (19%), SIRSI is used by four (15%), and DRA is used by three (12%). Six respondents (23%) use other vendors, which included Geac Advance, CDL and Melvyl, and EpixTech Horizon.

When access is managed by passwords and user IDs, passwords are typically randomly generated and are not expired on a regular schedule. The 40 responses to the question on how often passwords are expired showed evident confusion about the process. In several instances, there was no

mechanism in place to expire passwords, and they thus did not expire or expired "rarely" or with "no set period," although one respondent indicated that this was under review. Several respondents indicated that passwords expired at a fixed time—at the end of each quarter, semester, term, or annual session—but several also indicated that expirations were dependent on the status of the individual, and that expirations occurred when the person graduated or left the University.

There are a variety of schemes in place to prevent the hijacking of user IDs and passwords by unauthorized persons, including SSL and IP restriction to webpages that list passwords. There are also various methods for authentication when the initial user ID and password are assigned: for example, in-person registration with photo ID. Nonetheless, there appear to be no technical schemes for limiting the distribution of user IDs and passwords by authorized users to unauthorized users. Most institutions that recognized the existence of this problem have a use policy or honor system.

There are few respondents who manage access through a library gateway such as WebZ. Four of the 13 respondents (31%) use OCLC products such as WebZ and SiteSearch. The others use a webscript from OCLC, DRA Web2, VTLS, WebVoyage, or Voyager. Slightly fewer than half of this group has a gateway that provides access to both Z39.50 and non-Z39.50 resources. Only five respondents report that they manage access by digital certificates. Two of these use Kerberos and two use VeriSign.

The future of access management systems appears to indicate some turmoil. Of 47 respondents, almost half (22, or 47%) indicated that they plan to switch to a different access management system within the next two years. The responses are heterogeneous and most respondents seem still to be in the planning stage. The new systems most often mentioned are EZproxy, digital certificates, and LDAP. Several respondents indicated that they had identified nothing, but that evaluations were being done. These changes would bear reexamination.

Conclusions

One of the inescapable conclusions to emerge from this survey is that research libraries do not appear to possess a common standard or a common vocabulary that can be used for measuring, describing, and communicating their holdings of networked information resources. This is evident from the disparate responses to the deceptively simple question involving the number of networked information resources made available to authenticated users. That the responses are so disparate certainly demonstrates that there is no agreement on the standard unit of analysis for measuring the concept of "networked information resource." Libraries that can provide statistics on books and serials have more difficulty counting electronic resources.[1]

Another conclusion emerges directly from the library responses to the application-level proxy rewriter. Those libraries that have implemented an application-level proxy rewriter are able to serve additional resources through it, offering more resources than those libraries that do not use the application-level proxy rewriter. The application-level proxy server occupies a more central position in the authentication system than mechanical proxy servers. Although relatively few users rely upon a credential-based system to provide network access and authentication, an optimum system might integrate a credential-based system and the application-level proxy rewriter, eliminating the need for a gateway access management system.

Apparently, the Z39.50 standard no longer plays a significant role in the way research libraries provide access to their networked information resources. When only 20% of the responding libraries use a Z39.50 capable ILS for authentication and when that authentication represents only 6% of authenticated usage in those libraries, it is safe to say that the standard is less relevant than it once was and is no longer the future for libraries in meeting the information needs of their users.

Confidentiality of library records appears to be addressed by the deletion of ID data from session information. Most libraries are addressing the ALA *Policy on Confidentiality of Library Records* by establishing a system where the ID data cannot be retrieved because they are not archived. We think

this phenomenon deserves further attention, and speculate that the ID data are in fact valuable and should be retained. It is perhaps a lack of trust in policies or a lack of confidence in technical security that has encouraged so many institutions to remove this data.

There was little homogeneity in the 37 responses to Question 14, which involved security measures to insure that passwords and IDs are not distributed inappropriately. Some respondents use manual (personal) ID checks and verifications; others attempt to create secure pages with special logins and PINs; still others attempt to link to databases (payroll, registration, human resources) and to verify validity with other systems before establishing an account. Passwords likewise are distributed in all possible ways, with some respondents offering immediate validation while others send personal mail containing the passwords. Once the passwords are distributed, most institutions rely upon honor codes and signed use agreements to limit further distribution of the passwords by authorized users to unauthorized users. That there is such little agreement in the ways in which authorized and unauthorized users can be determined would seem to necessitate additional research and further study of this subject.

Finally, there were a number of comments concerning the heterogeneity of the authentication systems. "Extremely heterogeneous network," "There are a lot of different authentication and authorization systems all around campus," "Question 4 was difficulty to answer since we often use a combination of methods for our authentication routines." And most tellingly, "We have three layers of authentication." There are both layered, integrated systems and those with different authentication systems for different services. The complicated authentication environment is a difficult picture to survey. It does seem clear that, at many libraries, system analysis is being applied to authentication schema, and efforts are being made to integrate disparate authentication systems into a layered or sequential approach.

[1] Editor's note: The E-Metrics project, one of the ARL New Measures Initiatives, is an effort to explore the feasibility of defining and collecting data on the use and value of electronic resources. Information about the project is available on the ARL website at <http://www.arl.org/stats/newmeas/emetrics/index.html>.

SPEC Kit 267
User Authentication

Survey Results

Until the advent of the World Wide Web and the concomitant development of global computer networks, most research libraries could provide access to their resources with few concerns about the status of those who sought the information or concerns that the information was restricted to certain classes of users. Developments in computer technologies have irrevocably altered library operations, and it is now the exceptional library that has not in some way responded to the challenges of authenticating and authorizing its users, particularly those users needing to access the library's systems and networked information resources from remote locations. Furthermore, licenses for networked information resources increasingly require authentication controls, as well as setting levels of authorization.

Authentication and authorization are complex access management processes that involve a verification of the identity and status of the user, the ways in which IP ranges are limited, the processes by which information technology support is handled, and the systems by which authentication information and authorization levels are maintained.

This SPEC survey is designed to examine the systems research libraries use to authenticate and authorize the users of their online networked information resources. For the purposes of this survey, authentication is defined as the process of determining whether someone or something is, in fact, who or what he or she is declared to be. Authorization is the process of giving someone permission to do or have something, including privileges of use (such as access to file directories, amount of allocated storage space, access to licensed electronic resources, and so forth). Networked information resources are defined as electronically accessible information resources (e.g., library or academically developed databases, university databases, commercial databases, full-text services, e-journals, etc.) funded or enabled by the library, which are made available to authorized users through an intentional and systematic network (LAN, WAN, dial-in, etc.).

This survey was designed by Terry Plum, Assistant Professor, Simmons Graduate School of Library and Information Science, and Richard Bleiler, Humanities Reference Librarian, University of Connecticut.

Please submit this survey and send the requested documentation by **July 6, 2001**. As always, individual responses to the survey will be treated confidentially.

Note: Fifty-two of the 121 ARL member libraries (43%) responded to the survey.

Background

1. Does your institution authenticate users of networked information resources? (n=52)

Yes	51	98%
No	1	2%

Authentication

2. Which user categories may be authenticated? Check all that apply. (n=50)

Staff	48	96%
Undergraduate students	46	92%
Graduate students	46	92%
Faculty	46	92%
Any onsite user	15	30%
Consortium members	7	14%
Local community members	7	14%
Alumni	5	10%
Other	14	28%

Please explain

Other categories include: Friends of the Library, extension faculty and students, selected department-sponsored guest accounts, university affiliates, affiliated institutions, and external clients.

3. How many networked information resources are made available to authenticated users? (n=49)

Responses ranged from 1 to nearly 24,000. Clearly, there is no agreement on the unit of measure for these resources.

4. What type of access management system does your institution use to authenticate users of networked information resources? Check all systems that are used. Indicate the number of resources available through each system used and the percent of total use each system receives. (Approximations are acceptable.) Also, check each system for which usage statistics are gathered and maintained. (n=51)

Type of System	Used	% of Total Use			Statistics gathered
		mean	median	n	
Credential-based System	**45**				
Password and User ID	40	38.2	10.0	20	11
NetID	8	38.0	11.0	3	4
Public Key Infrastructure	3	—	—	0	1
Smart Card	1	—	—	0	0
Proxy System	**36**				
Mechanical proxy (Pacfile)	26	59.8	60.0	11	7
Application-level proxy(Rewriter)	12	75.5	87.3	8	6
IP Source Address Filtering	**42**				
IP with proxy server	29	78.1	89.0	9	7
IP with no proxy server	25	58.2	60.0	9	5
IP with modem pool	17	37.5	18.0	5	1
Dynamic IP address	13	60.0	70.0	7	4
Reverse DNS look-up	4	50.5	50.5	2	0
Library Gateway	**12**				
ILS with Z39.50	10	6.0	6.0	1	1
non-ILS such as WebZ	4	52.5	52.5	2	0
Referral URL	**7**	35.5	20.5	4	1
Other System	**4**	36.6	5.0	3	2

5. How does the authentication system verify eligible users? (n=51)

System checks against a dynamic database within ILS	28	55%
System checks against a dynamic institutional personnel database	20	39%
System checks against a flat file extracted from ILS	14	28%
System checks against a separately created database of eligible users	14	28%
System checks against a flat file extracted from the institutional personnel database	7	14%
Other	5	10%

Please explain

Other responses include: Virtual Personal Network (VPN) and personal certificates.

Authorization

6. Which networked resources and services may an authenticated user access? Check all resources and services that apply for each type of authentication system. (n=51)

	Credential-based System	Proxy System	IP Filter	Library Gateway	Other System
Personal circulation record	35	1	0	3	3
Request ILL/DD	33	3	3	1	3
Email	33	2	0	0	2
Place holds/recalls on books	31	0	0	4	3
Course registration info	29	2	0	0	4
Databases	28	41	42	8	2
Course reserve materials	25	14	14	4	2
File space on network server	25	0	0	0	2
Financial records	21	2	0	1	4
Computer labs	21	0	0	0	3
e-books	20	36	35	3	3
e-journals	20	40	39	3	2
Library OPAC	19	11	10	9	3
Distance education courses	18	6	3	0	2
Transcripts	17	2	0	0	4
Photocopy machines	7	0	0	0	5
Dining facilities	7	0	0	0	5
GroupWare	7	0	0	0	2
Other	5	1	0	0	1

Please explain

Credential-based systems are also used to provide access to printers and staff webpages.

User Privacy

7. How does the access management system handle user privacy? (n=49)

Anonymous access (Each session is anonymous. Repeat users cannot be identified.)	32	65%
Identified access (Actual identities are associated only with sessions.)	24	49%
Pseudonymous access (Repeat users can be identified, but the identity of a user cannot be determined.)	12	25%
Identified access and data are archived	10	20%
Pseudonymous access with demographic identification (Demographic characteristics of users can be determined, but not actual identities.)	8	16%
Other	1	2%

Please explain

Various authentication systems log limited user session information. Details of user activity are not kept.

System Management

8. Who manages the authentication and authorization system(s)? Check all that apply. (n=51)

Central library information technology (IT) staff	46	90%
Institution or campus-wide IT	37	73%
Vendor of networked information resource	25	49%
Consortium IT	5	9%
Branch or regional library IT	2	4%
Outsourced to a noninstitutional IT group	0	0%
Other	4	8%

Please explain

The other responses explained the overlap in management.

System Specific Questions

If access to networked information resources is managed by IP:

9. Now many available resources are managed at the: (n=37)

Vendor level
Consortium level
Institution level
Other

As with Question 3, respondents had a hard time answering this question. A general impression is that the vendor most often manages this access.

If access is managed by IP and a proxy server:

10. What is the proxy server software? (n=46)

EZ Proxy	15	33%
Squid	8	17%
Web Access Management (III)	6	13%
Netscape iPlanet Proxy	3	6%
Microsoft Proxy	1	2%
Other	13	28%

Please explain
The other software most often mentioned was Apache. Muffin and custom solutions were also mentioned.

If access is managed by an ILS using Z39.50:

11. Which ILS does your institution use? (n=26)

Endeavor	5	19%
III	5	19%
CIRSI	4	15%
DRA	3	12%
ExLibris	2	7%
NOTIS	1	4%
Other	6	23%

Please explain
Other ILS vendors include: GEAC, California Digital Library, and EpixTech.

If access is managed by passwords and user IDs:

12. How are passwords and IDs generated? (n=43)

In general, passwords are randomly generated.

13. How often are they expired? (n=40)

In many cases, passwords expire when the individual leaves the institution. In some cases, they expire at a set time, such as the end of the quarter, semester, term, or year.

14. What security measures are used to insure that passwords and IDs are not distributed to ineligible users? (n=37)

The majority of respondents indicated that staff checks an institutional or other valid ID before assigning a password to a user. Often, users are then required to sign a form that describes how passwords are to be used and what sanctions are possible for misuse. In cases where passwords are placed on a website, the user has to enter ID information similar to the in-person verification before they can access the file.

If access is managed by a library gateway such as WebZ:

15. Which gateway software does your institution use? (n=13)

WebZ	3	23%
Launcher	0	0%
Other	10	77%

Please explain

Other responses include: a webscript from OCLC, DRA Web2, VTLS, WebVoyage, and Voyager.

16. Does the gateway provide access to both Z39.50 and non-Z39.50 resources? (n=12)

Yes	5	42%
No	7	58%

If access is managed by digital certificates:

17. Which system does your institution use? (n=5)

Kerberos and VeriSign were the two systems mentioned.

Future Plans

18. Does your institution plan to switch to a different access management system within the next two years? (n=47)

Yes	22	47%
No	25	53%

If yes, please identify the proposed new system. (n=22)

EZproxy, digital certificates, and LDAP were most often identified, those most respondents appear to be in the planning stage and have not decided on the next system.

Responding Institutions

University of Alabama
University of Alberta
Boston College
Brigham Young University
University of British Columbia
University of California–Davis
University of California–Irvine
University of California–Riverside
University of California–San Diego
Canada Institute for Scientific and Technical Information
University of Colorado
Colorado State University
University of Connecticut
Cornell University
Dartmouth College
Duke University
University of Florida
University of Guelph
University of Hawaii
Indiana University
University of Iowa
Johns Hopkins University
University of Kentucky
Laval University
Library of Congress
Louisiana State University
McMaster University
University of Manitoba
University of Massachusetts
Massachusetts Institute of Technology
Michigan State University
University of Minnesota
University of Nebraska–Lincoln
University of New Mexico
University of North Carolina
University of Oklahoma
University of Oregon
Purdue University
University of Rochester
State University of New York at Albany
State University of New York at Buffalo
University of Tennessee
University of Virginia
Virginia Tech
University of Washington
Washington State University
Washington University
University of Waterloo
Wayne State University
University of Western Ontario
York University

SPEC

Representative Documents

Explanations for Users

UNIVERSITY OF ALBERTA

http://www.library.ualberta.ca/remote/index.cfm

University of Alberta Libraries

Home | Catalogue | Databases | e-Journals | Subject | Services | About Us

Français
Text Version

Location: Home > Remote Access **Wednesday December 12, 2001**

Additional Information

- Services for Distance Students
- Other Access Options

Off Campus Access to Electronic Library Resources

Many of the resources on the University of Alberta Library website require anyone using an internet service provider other than the University of Alberta or the U of A/TELUS modem pools to "authenticate" themselves through the **University of Alberta Proxy Server** prior to usage.

(For example, if you are connecting to the internet via CompuSmart, Shaw, TELUS ADSL, SprintNet, OANet or other similar internet service providers, you will have to use the proxy server.)

Additional Help

The University of Alberta Proxy Server is a service of Computing and Network Services. If you need help configuring the proxy server, please contact the **CNS Help Desk**.

If you would like to speak with a HelpDesk consultant in person, please phone 492-9400, stop by Room 302, GSB or **E-Mail the HelpDesk**.

To access a web-based resource using the proxy server, users must configure their web browser as outlined on the browser-specific pages listed below. "Re-authentication" is required every thirty minutes.

- **Instructions for Netscape 4.x**
- **Instructions for Netscape 3.x**
- Instructions for Internet Explorer 4.x (Telephone Modem/56 K or slower)
- Instructions for Internet Explorer 4.x (High Speed Cable or ADSL connections)
- Instructions for Internet Explorer 5.x (Telephone Modem/56 K or slower)
- Instructions for Internet Explorer 5.x (High Speed Cable or ADSL connections)

- Instructions for Macintosh Users

Learning Systems University of Alberta | Index | Sitemap | Contact Us

Access to UC Davis Licensed Resources

Using a non-UC Davis (includes DSL providers) Internet Service Provider

For UC Davis faculty, students, and staff only who have a UCD Login ID and password.
(If you use a UC Davis network address, you **DO NOT** need to use the proxy server.)

Instructions for setting up your browser to use the proxy:	
Using Windows:	**Using a Macintosh:**
Using Netscape 3.x	Netscape v.3.x
Using Netscape 4.x	Netscape v.4.x
Note that Netscape 6.x does not support automatic proxy configuration on either platform	
Using Internet Explorer 4.x	**Note that Internet Explorer for the Macintosh does not support automatic proxy configuration**
Using Internet Explorer 5.x	

Best configuration for using the library's proxy server:

Netscape: version 4.77
IE: version 5.5 with service pack 1 + May 24 security patch

Please Note:

Some resources may not function properly when accessed through the proxy server. A list of these resources is maintained. If you experience problems with a particular resource, please check the list.

Connecting through AOL: you will need to use Netscape as your browser while using the UC Davis Proxy Server.

If you are using an Internet Service Provider (ISP) that uses a firewall, please contact your ISP systems administrator to determine how best to connect to the UC Davis General Library proxy server. If your ISP systems administrator would like to consult the library's proxy server specialist, please call (530) 752-1202 or email techhelp.

NOTE: Specific cache settings are required for IE and Netscape.

Make sure that your browser is set to verify documents every time, and that the cache is cleared.

Before you can use the proxy server from your web browser, you must have a UCD LoginID and password. The proxy server authenticates users before acting as their agent, so you will be asked for your UCD LoginID and password whenever your browser accesses a resource through the proxy server.

Important steps to complete!

If you do not have a UCD LoginID, use the instructions found at http://mothra.ucdavis.edu/services/ . To get further help in setting up access, faculty and staff should contact their departmental Technical Support Coordinators (TSCs); students should contact IT Express at 754-HELP.

If you do not know whether you have a valid UCD LoginID, follow the instructions on the web-based Mothra Services Menu at https://mothra.ucdavis.edu/services/.

If you have forgotten your password, go to IT Express in Shields Library in person with a picture ID to change it.

UC Davis Medical Center personnel: if you do not have a UCD LoginID or have questions about using the proxy, contact Rick Lawler (nck.lawler@ucdmc.ucdavis.edu) or Neil Knoblock (neil.knoblock@ucdmc.ucdavis.edu) in UCDMC Information Services.

Warning:

Once you have established a proxy configuration for your browser, every URL that you select will be checked first with the proxy. If there are network difficulties in reaching the proxy, you may not be able to connect to any URL. When this happens, you will need to disable the use of the proxy by your browser.

Questions, Problems?

If you have questions or experience problems using the Library's proxy service, please contact a reference librarian.

What is a web proxy server?

A proxy server is used as an intermediary between a web browser requesting a URL and the server that stores the URLs of restricted access resources. Valid users of domain restricted material using non-UC Davis networks, must configure their browsers to use the proxy service (see instructions above). Whenever such users attempt to retrieve restricted resources, the proxy server acts as an agent, retrieving the material and then re-transmitting it to the user. The proxy server authenticates users before acting as their agent. Currently, this authentication relies on the campus Kerberos service.

More information can be found in the IT Times article "Electronic Library Resources Now Available Anywhere."

The University Library (530)752-1202
University of California, Davis, 100 N.W. Quad, Davis CA 95616

send comments to Web Design Team
Page last updated 6 August, 2001

The UCI Libraries

University of California, Irvine

Home | ANTPAC | CDL/MEL | Hours | Search | New | Resources A-Z | Resources by Subj or Coll | Services | About | Internet

Connecting from home: remote access guide (UCI students, faculty, and staff only)

Choose an option below to have access to all UCI Libraries licensed resources:

- **ISP users - UCI Proxy Server -- more detailed instructions**
  - Access to UCI Libraries licensed resources for those using a non-UCI Internet Service Provider such as Cox@Home, AOL, or Earthlink
  - UCInetID and password required
  - One time only web browser proxy configuration needed
- **ZOTnet -- more detailed instructions**
  - Low cost Internet Service Provider only for UCI
  - UCInetID and password required
  - No web browser proxy configuration needed to use UCI Libraries licensed resources
- **UCI LifeLine Modem Service -- more detailed instructions**
  - **Limited** (time constraints), free dial-up access to the UCI campus network and the Internet. Not intended for more than modest needs.
  - UCInetID and password required
  - No web browser proxy configuration needed to use UCI Libraries licensed resources
- **CDL/MELVYL® passwords** (alternative for remote access to CDL-hosted databases purchased by UCI Libraries)

ISP users - UCI Proxy Server

Enables access to UCI Libraries licensed resources for those using a non-UCI Internet Service Provider such as Cox@Home, AOL, or Earthlink. **UCI LifeLine Modem Service** and **Zotnet** users do not need to use the Proxy Server.

1. You must have an active UCInetID to use the UCI Proxy Server. Activate your UCInetID by following the instructions on the Network & Academic Computing Services (NACS) page, **http://www.nacs.uci.edu/ucinetid/index.html**.
2. Configure your browser following the instructions on the NACS page, **http://www.nacs.uci.edu/help/proxy/**.
3. After you configure your browser, return to the UCI Libraries Web site and click on the names of the UCI resources you wish to access.
4. If prompted, enter your UCInetID and password. You will be connected to all resources as though you were on campus.
5. More information on the UCI Proxy Server is available at the NACS page, **http://www.nacs.uci.edu/help/proxy/**.

- *See* - **CDL passwords** for an alternative to the UCI Proxy Server for access to CDL-hosted databases purchased by UCI Libraries.

ZOTnet Internet Service

ZOTnet is a custom tailored, low cost Internet Access Service provided by zNET Internet Services for UCI students, faculty, and staff exclusively.

1. You must have an active UCInetID to subscribe to ZOTnet. Activate your UCInetID online by following the instructions on the Network & Academic Computing Services (NACS) page, **http://www.nacs.uci.edu/ucinetid/index.html**.
2. Connect thru ZOTnet. For more information on ZOTnet and how to subscribe, *see* - **http://www.zotnet.net/**, or contact OAC (949) 824-6116.
3. Return to the Libraries Web site and you will be able to access resources as though you were on campus.

- *See* - **CDL passwords** for an alternative to ZOTnet for access to CDL-hosted databases purchased by UCI Libraries.

UCI LifeLine Modem Service

Limited (time constraints), free dial-up access to the UCI campus network and the Internet. Not intended for more than modest needs.

1. You must have an active UCInetID to use the UCI LifeLine Modem Service. Activate your UCInetID online by following the instructions on the Network & Academic Computing Services (NACS) page, **http://www.nacs.uci.edu/ucinetid/index.html**.
2. Connect thru the modem service following the instructions on OAC's page, **http://www.nacs.uci.edu/communication/modems/**.
3. Return to the Libraries Web site and you will be able to access resources as though you were on campus.

- *See* - **CDL passwords** for an alternative to the LifeLine Modem Service for access to CDL-hosted databases purchased by UCI Libraries.

[top of page]

CDL -- **California Digital Library/MELVYL® passwords**

CDL/Melvyl® passwords provide an alternative for remote access to CDL-hosted databases (formerly called Melvyl® databases) purchased by UCI Libraries. CDL-hosted databases are available on the **CDL/Melvyl® page**.

There are certain advantages to using a password to access these databases:
- no need to configure your web browser
- useful for world travellers/researchers
- allows access from public computers at other universities or libraries

CDL passwords allow authorized users access to the database information, but not necessarily to all the full-text articles linked in the database references. More information on CDL passwords is available at the **California Digital Library**.

Passwords are available to **UCI faculty, students, and staff only**. You may obtain a CDL password at the following locations:

Main Library:
Multimedia Resources Center (MRC)
Email: mrc@uci.edu
Phone: (949) 824-7072

Science Library:
Interactive Learning Center (ILC)
Email: ilc@uci.edu
Phone: (949) 824-3680

Medical Center Library (MCL)
Email: mclref@uci.edu
Phone: (714) 456-5585

UCI -- **This resource is available to UCI users only**

On-campus access:
- UCI Libraries licensed resources are available from any computer with a direct Ethernet connection to the UCI network (i.e., any computer with a UCI IP address) including computers in the UCI Libraries and in campus buildings and offices.

Off-campus access via:
- **ISP users - UCI Proxy Server**
- **ZotNet**
- **LifeLine Modem Service**

Authentication with a valid UCInetID is necessary to use these services.
(Non-UCI users are not permitted remote access to these databases due to licensing agreements with the resource providers.)

CDL-Hosted Databases purchased by UCI Libraries may also be accessed from off-campus by UCI faculty, students, and staff using a **CDL password** as an alternative.

-- **Open to the world**

Access to this resource is unrestricted and open to all Internet users.

[top of page]

UNIVERSITY LIBRARIES

REMOTE ACCESS

Remote Access to Chinook: CU-Boulder Students, Staff, and Faculty

To use Chinook databases from off-campus, we recommend you log on using your CU IdentiKey. However, if you are using an Internet Service Provider other than CU-Boulder (for example, US West, AOL, Earthlink), you must configure your web browser to use our proxy server in order to gain full access to Chinook databases. Using your IdentiKey or the proxy server allows the Libraries to recognize that you are an authorized CU student, staff, or faculty member.

Connecting to CHINOOK using IdentiKey and campus modem pools:

Off-campus access to Chinook, the Libraries' online catalog, and all gateway services (including Article Access databases) is available free to CU-Boulder students, faculty, and staff by dialing into the campus network via the PPP/SLIP modem pool. An IdentiKey password is needed to make the connection.

1. Obtain an IdentiKey password and Internet software (if needed) from Information Technology Services (ITS).
2. Set your modem software to dial the appropriate phone number:

   Off-campus: **303-218-8000**

   Family Housing: **4-9900**

3. Configure your modem software so that it enters your campus username and IdentiKey password when a connection to the modem pool is made.
4. Once connected to the campus modem pool, open a Web browser (Netscape, Internet Explorer, etc.)
5. In the Location box, type the URL for Chinook: http://libraries.colorado.edu

For more information about establishing a connection to the campus network from off-campus, see the Information Technology Services (ITS) web page at http://www.colorado.edu/ITS/docs/#comm or call the ITS Service Center at 303-735-4357.

Connecting to CHINOOK using commercial Internet Service Providers (ISPs):

If you are using an Internet Service Provider other than CU-Boulder (for example, US West, AOL, Earthlink), you must configure your web browser to use our proxy server. Using the proxy server allows the Libraries to recognize that you are an authorized CU-Boulder student or employee. After you configure your browser and click on a link to one of our commercial databases, you will be asked to complete a verification form that looks like this. Once you have completed this form, all of your Internet activity will be routed through our proxy address until you turn off the proxy setting on your web browser.

Please note:

- Due to a limited amount of space on our proxy server, we are unable to include individual online journals available through Chinook. To access these journals, log on using your Identikey. This will allow full access to **all** online databases.
- Remember to de-activate the proxy when you do not need it. Otherwise your browser's response time and/or ability to reach other desired web sites might be affected.
- There has been a much higher success rate using the proxy with Netscape Navigator than with Internet Explorer. If you have trouble with Internet Explorer, you may want to try using Netscape Navigator.

BEST COPY AVAILABLE

Proxy Server Configuration

Netscape Version 3

1. Select **Options**
2. Select **Network Preferences**
3. Select the **Proxies** tab
4. Enter in the **Configuration location** (URL):
http://libraries.colorado.edu:8080/proxy.pac
6. Click **Reload** and **OK**

Netscape Version 4

1. Select **Edit** from the pull-down menu at the top of the screen
2. Select **Preferences**
3. Click on the "+" to the left of the **Advanced** option
4. Click on **Proxies**
5. Click on the **Automatic proxy configuration** button
6. Enter in the **Configuration location** (URL):
http://libraries.colorado.edu:8080/proxy.pac
7. Click **Reload** and **OK**

MS Internet Explorer Version 3.02

1. Select **View**
2. Select **Options**
3. Select the **Advanced** tab
4. At the bottom of the **Advanced** page, click on the **Automatic Configuration** button
5. Enter in the URL:
http://libraries.colorado.edu:8080/proxy.pac
6. Click on **Refresh** then click on **OK** in the popup box
7. Click on **Apply** then **OK** on the **Options** menu

MS Internet Explorer Version 4

1. Select **View**
2. Select **Internet Options**
3. Select the **Connection** tab
4. In the **Automatic Configuration** box clik on **Configure**
5. Enter in the URL:
http://libraries.colorado.edu:8080/proxy.pac
6. Click on **Refresh**
7. Click on **OK** then **OK** again on the **Internet Options** menu

MS Internet Explorer Version 5

Dial-up Modem Connection

1. Select **Tools**
2. Select **Internet Options...**
3. Select **Connections**
4. In the **Dial-up settings** box find the icon with the name of your dial-up service. Click on the icon once to highlight it.
5. Select: **Settings...**
6. Check the box next to: "**Automatically detect settings**"
7. Check the box next to: "**Use automatic configuration script**"
8. Enter this Address:
http://libraries.colorado.edu:8080/proxy.pac
9. Click on **OK**
10. Click on **OK** on the **Internet Options** menu

Local Area Network (LAN) connection

1. Select **Tools**
2. Select **Internet Options...**
3. Select **Connections**
4. Select : **LAN Settings**
5. Check the box next to: "**Use automatic configuration script**"
6. Enter this Address:
http://libraries.colorado.edu:8080/proxy.pac
7. Click on **OK**
8. Click on OK on the **Internet Options** menu

Notes for AOL Users

AOL's Web Browser will not work with our proxy server. You will need to use Netscape Navigator while connected to your AOL account. To install Netscape Navigator for AOL:

1. Run the America Online Program
2. Keyword: **netscape**
3. Click on **Click Here!**
4. Click on **Download Netscape**
5. Follow the prompts to load and install Netscape Navigator
6. Follow the steps listed above for setting up Netscape Version 4

Remember to de-activate the proxy when you do not need it. Otherwise your browser's response time and/or ability to reach other desired web sites might be affected.

Colorado State University Libraries Home

Library Catalog (SAGE) | Databases | Interlibrary Loan | Search the Web | Help | CSU

Remote Access to Library Databases: Proxy Server Instructions

Proxy Server
Frequently Asked Questions
Off-Campus Access
Help
Distance Users

To use Libraries databases and electronic journals from off campus, you must:

1. Tell your Web browser to use our proxy server.
2. Be a *currently enrolled* CSU student or a CSU employee.
3. Have either Netscape Navigator/Communicator 3.0 or 4.x, or Microsoft Internet Explorer 4.0 or 5.0. Unfortunately, Netscape 6.0 and Internet Explorer 5.5 do not work.

Some Internet Service Providers do not work with our proxy server. Read our notes for:

- America Online
- Compuserve
- NetZero

With your Web browser configured, select a database from our list. You should see a login screen exactly like this. If not, you have not configured your browser properly.

Setup Instructions.

Troubleshooting Wizard

Test your Web browser

Download Netscape Navigator Stand-alone, which works with our proxy server.

How the proxy server works.

Content: Distance Learning Team

Last updated: 10/30/01
URL: http://lib.colostate.edu/distance/proxy.html

A-Z Index

Colorado State University Libraries ◆ Colorado State University Library Catalog (SAGE) ◆ Databases ◆ Interlibrary Loan ◆ Search the Web ◆ Help

Disclaimer & Copyright Statement

How the Proxy Server Works

Proxy Server
Frequently Asked Questions
Off-Campus Access
Request Articles & Books
Research at a Distance
Help
Home
Other Libraries

Why we use a proxy server:

The databases provided by CSU Libraries are on the Web but are **not** free. We purchase these from companies. Our agreements with them limit access to CSU employees and registered students. If you are not on CSU's campus, the database companies do not know that you are affiliated with the university, so you are denied access.

How the proxy server works:

The proxy server is a computer in Morgan Library. Once you configure your web browser to use it, this is what happens...

- You click on a link to a database.
- Your computer tells the proxy server it wants to use a database.
- The proxy server asks you to give your name, CSU ID number, and a PIN number that you create the first time you are asked.
- The proxy server looks you up in the Libraries' circulation system.
- If you're in the system, the proxy server acts as a mediator between you and the database.
- The database will talk to the proxy server, which it knows is on the CSU campus.
- The proxy server takes information from you, talks to the database, then sends information from the database back to you.

Once you've logged in to the proxy server, you cannot see the rest of this happening. It just seems like you're talking to the database directly.

How the proxy server works:
(in pictures)

- Database access without the proxy server
- Database access with the proxy server

Content: Distance Learning Team

Last updated: 10/30/01
URL: http://lib.colostate.edu/distance/proxy_explain.html

A-Z Index

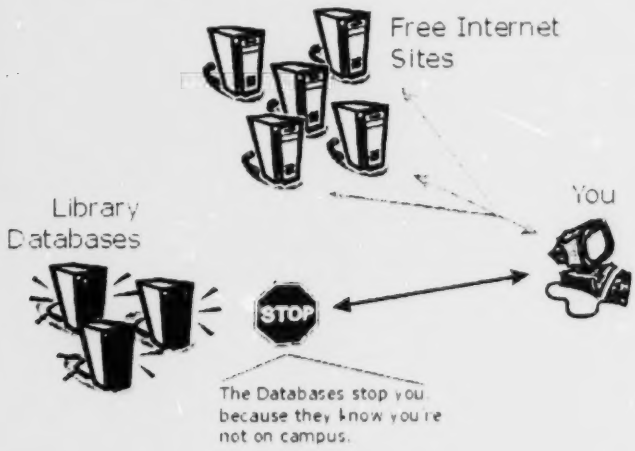
Colorado State University Libraries ◆ Colorado State University Library Catalog (SAGE) ◆ Databases ◆ Interlibrary Loan ◆ Search the Web ◆ Help

Disclaimer & Copyright Statement

Without the Proxy Server

Proxy Server
Frequently Asked Questions
Off-Campus Access
Request Articles & Books
Research at a Distance
Help
Home
Other Libraries

When you're not using the proxy server, this is roughly what happens:



- Your computer talks freely to most sites and computers on the Internet.
- When you try to talk to a computer where one of the databases lives, you get turned away.

To see what happens with the proxy server...

Content: Distance Learning Team

Last updated: 10/30/01
URL: http://lib.colostate.edu/distance/noproxy.html

A-Z Index

Colorado State University Libraries ◆ Colorado State University Library Catalog (SAGE) ◆ Databases ◆ Interlibrary Loan ◆ Search the Web ◆ Help

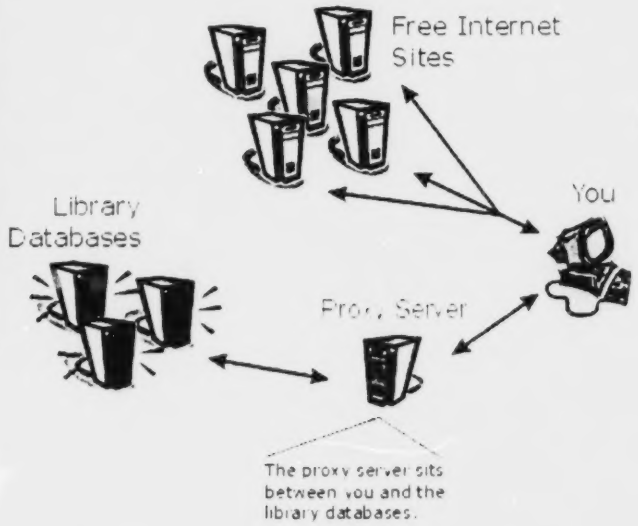
Disclaimer & Copyright Statement

BEST COPY AVAILABLE

With the Proxy Server

Proxy Server
Frequently Asked Questions
Off-Campus Access
Request Articles & Books
Research at a Distance
Help
Home
Other Libraries

When you're using the proxy server, this is roughly what happens:



- Your computer talks freely to most sites and computers on the Internet, and the proxy server doesn't interfere.
- When you click on a link to a database, your computer knows it has to make a request to the proxy server.
- All communication between you and the database flows through the proxy server.

Back to how the proxy server works.

Content: Distance Learning Team

Last updated: 10/30/01
URL: http://lib.colostate.edu/distance/withproxy.html

A-Z Index

Colorado State University Libraries ◆ Colorado State University Library Catalog (SAGE) ◆ Databases ◆ Interlibrary Loan ◆ Search the Web ◆ Help

Disclaimer & Copyright Statement

BEST COPY AVAILABLE

University of Connecticut

University Information Technology Services

Obtaining an account on the University of Connecticut Proxy Server

Overview

Proxy accounts allow access to web-based resources that are normally restricted to those using a valid UConn IP address (internet numeric addresses starting with 137.99). Accounts on the proxy server can be obtained by faculty, staff, and students at the University of Connecticut.

If you are using an Internet Service Provider such as MSN, Earthlink, SNET, AT&T, etc., you will not be able to access restricted services. Using a proxy account provides a solution.

NOTE: Proxy Services work best with Netscape Navigator/Communicator. Proprietary browsers that come bundled with certain Internet Service Providers (such as AOL, Compuserv & Prodigy) **cannot** be configured to use Proxy. Also, some versions of Internet Explorer cannot be configured for automatic proxy.

Some examples of resources that are limited by IP are:

1. Many UConn Library resources http://www.lib.uconn.edu, including Electronic Course Reserve http://www.lib.uconn.edu/ECR, most databases http://norman.lib.uconn.edu/NewSpirit/Databases, and electronic journals, http://norman.lib.uconn.edu/NewSpirit/FullText, due to contractual and licensing agreements.
2. UConn Software Distribution Server (ftp.uconn.edu) http://ftp.uconn.edu through the web, due to site license restrictions.
3. IBM BookManager® BookServer Library http://docs.uconn.edu/cgi-bin/bookmgr/bookmgr.cmd/library.

If your workstation is already within the UConn.edu or the Uchc.edu domain, it should not be set to use the proxy server.

Workstations are in the UConn.edu or Uchc.edu domains if they are:

1. Physically located on the University of Connecticut campuses, including Storrs, the Regional campuses, the Law School, and the Health Center.
2. Using the UConn mainframe
3. Using the Univ. ITS PPP Internet Service http://vm.uconn.edu/~wwwppp

Getting an Account

Currently a userid and a password is required for using the proxy server. Application forms for obtaining accounts can be obtained in the Univ. ITS Accounts Office, in Room M001 in the Math Science Building.

There is a single application form for faculty, students and staff, available online. It **cannot** be filled out electronically. It **must** be printed, and then filled out by hand. Application forms can be returned via mail, campus mail, or fax(486-4131). The Accounts Office can be reached by phone at 486-5236.

If mailing from campus, the address is:

```
Univ. ITS Accounts
Unit 3138
```

If mailing from outside campus, please use this address:

```
Univ. ITS Accounts
196 Auditorium Road, Unit 3138
University of Connecticut
Storrs, CT 06269-3138
```

Finally, if you want to fax your completed form, please use this number:

```
860-486-4131
```

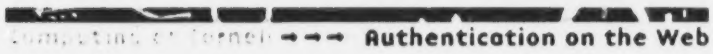
Forgotten passwords

If you forget your password, you will have to contact the Accounts office, at 486-5236, in Room M001 in the Math. Sci. Bldg. You may be required to come in person and show identification.

In order to access any IP restricted, web-based resources, a proxy server must be configured within your web browser. Instructions for setting up your browser can be obtained by clicking here.

Go to Top

This page is maintained by The University of Connecticut
Information Technology Services Help Desk



Proxy Server

for Access to Library Resources from Outside Cornell

- What is a proxy server?
- Do you need to use the proxy server?
- How to use the proxy server
- Frequently asked questions
- Troubleshooting

What is a proxy server?

Access to some online resources, such as the Library Gateway's periodical indexes, is limited to Cornell students, faculty, staff, and affiliates. Depending on how you connect to the network, you may or may not be recognized as a member of the Cornell community entitled to use these resources.

The proxy server solves this problem by acting as your authorized agent: It confers with other servers (Cornell's Kerberos and permit servers) to verify that you are entitled to view the materials you have requested, then requests the materials for you. Because the proxy server has a Cornell network address (proxy.cornell.edu), it is automatically recognized as an authorized Cornell user and so is allowed access to the materials you have requested.

Do you need to use the proxy server?

You **don't** need to use the proxy server if you connect to the Internet through Cornell. Cornell connections include direct-wired connections from campus buildings (ethernet or ResNet), or either of the Cornell dial-up services (EZ-Remote or Express Lane).

You **do** need to use the proxy server if you connect to the Internet using any other Internet service provider, such as RoadRunner.

How to use the proxy server

To begin using the proxy server, follow the steps listed here. Once you have everything set up, you will not need to take any special steps each time you need access to a restricted resource through the proxy server. Your Web browser will automatically contact the proxy server when it is needed.

Note: At present it is not possible to use the proxy server with Internet Explorer on Macintosh (see note). You need to use Netscape on a Macintosh, or either Netscape or Internet Explorer on Windows.

The proxy server also does not work with Netscape 6 on either Macintosh or Windows.

1. Have Kerberos and SideCar security software installed and running on your computer. On Windows, if SideCar is running you'll see a key icon near your Start menu button. On Macintosh, pull down the Applications menu (upper right corner of your screen) to see if SideCar is running. If you don't have this software, use one of these links to get it:
   - Download Bear Access, including Kerberos and SideCar
   - Download Kerberos and SideCar without Bear Access
   - More about Kerberos and SideCar
2. Set up your web browser to use two features: cookies and automatic proxy configuration. Instructions are provided separately for the most popular web browsers:
   - Netscape
   - Internet Explorer
3. Use your Web browser normally.
4. When you select a restricted page, you will receive the usual Kerberos prompt for your Net ID and password, unless you already have an active Kerberos ticket. Your password will be encrypted by Kerberos for safe transmission over the network.
5. You don't need to turn proxying off when you're done using library databases; you can simply leave it active all the time. Your browser will only use the proxy server for a very specific list of Cornell-restricted sites, while all other transactions will occur normally.
   If you do want to turn this feature off for any reason, follow the same instructions linked in Step 2 to locate the window where

the Cornell proxy server's address is recorded, then remove the address, leaving the field blank.

Frequently Asked Questions

- Who is authorized to use the CU Library Gateway?
- How can I use the resources on the Library Gateway ...
  - when I travel or when I use a computer without Bear Access?
  - if I don't use EZ-Remote as my Internet Service Provider?
  - if I use UNIX?

Troubleshooting

- Proxy Server Errors (info from the Library Gateway)
  - Why can't I get into the Cornell restricted databases through the Library Gateway?
  - I have set up a proxy server according to instructions but it still doesn't work. What can I do?
  - When using Internet Explorer 5, I occasionally get an IP Check Failed error. What do I do?
  - While trying to enter a resource on the Gateway, I was asked for a special login and password. Is this right?
- Authentication and SideCar Errors (info from the Library Gateway)
  - Why do I have to occasionally use SideCar when I use a Cornell restricted database?
  - Why do I get a Proxy Authentication Error?
  - Even though I have SideCar and Bear Access running, I received the error message "Checking authorization by Cornell NetID...failed. Check that SideCar is running on your computer and try again". What should I do?
- Authentication and SideCar Errors (info from the CIT HelpDesk)
  - Windows
  - Macintosh
- Library Gateway Computer Set-up page
- Library Gateway FAQ: Resolve Errors and Common Technical Questions
- Library Gateway Technical Problem Report Form

Introduction | Netscape | Internet Explorer | Technical Info

Computing at Cornell ➡ CIT Services ➡ Kerberos and SideCar ➡ Proxy Web Server

Last modified: October 11, 2001
Need help? Please use the Library Gateway's Technical Problem Report Form
Comments about this web page: cit_pubs@cornell.edu

Kerberos Authentication at Dartmouth

This series of web pages include an explanation of how this software works, installation instructions for various hardware platforms, an authentication test page, hints for WWW developers and who to contact if you have trouble installing this software. You can download the kerberos software directly from these web pages.

Many network services depend on being able to identify users of a system in order to limit access. For example you login to your electronic mailbox with a userid and password so only you can read your mail. Many databases are licensed from commercial publishers who require their use be restricted to a specific license holder. Kerberos authentication software enables us to restrict access to our licensed applications.

The following are some examples of the applications that use this software for access:

- DA$H card balances (Dartmouth users only)
- Degree audit (Dartmouth users only)
- DCIS via the WWW (Dartmouth users only)
- Biomedical Databases via Ovid (Dartmouth and Dartmouth-Hitchcock users)

HINT: Always use the Testing your Installation page to verify that your Kerberos installation was done correctly.

- How it Works
- Install Configurations
  - Macintosh
  - Windows 95/98/2000 and Windows NT (32-bit)
  - Unix
- Clearing your Kerberos Ticket
- Testing your Installation
- Problem Resolution (trouble-shooting)
- Information for Web Page Developers
  - Using Kerberos in Perl CGIs
  - Using Kerberos to Restrict Access to a Web Page

Additional questions? Send email to the Computing Services Help Desk
Last modified on 08/14/01 by MML
©2001 Trustees of Dartmouth College

DARTMOUTH COLLEGE

http://www.dartmouth.edu/~kerberos/intro.html

Kerberos Authentication
How it Works

To use licensed databases from the Dartmouth web you need to install the Kerberos software on your desktop computer. The Kerberos software is comprised of two programs; you'll need to install the programs called KClient and SideCar.

These two software programs were developed originally at Cornell University to authenticate web page access. KClient and SideCar have been licensed for use at Dartmouth College and the Lahey Hitchcock Medical Center. You can obtain these programs through these web pages. After installation of these programs, you must restart your system to get the software running.

KClient

The KClient package combines your name and your computer's network address to produce an unforgeable network-wide authentication *ticket* . This electronic ticket can, in turn, prove to a remote server that you are the individual using a particular computer.

SideCar listens for authentication requests from a web server. If a ticket is available (eg. if a person has already authenticated with KClient), SideCar simply returns the ticket. If no ticket is available, SideCar asks KClient to present the authentication dialog, and then sends the resulting ticket back to the requesting web server.

This ticket is useful for a specified time, generally in the range of 5 minutes to several hours (you can set this expiration time yourself). After the lifetime of the ticket expires, you must re-authenticate yourself. This provides safety against someone using a ticket from a computer after you have stopped using it. It is important that you close your ticket, especially on a public machine or a machine that you share with other users.

SideCar

SideCar is an application that permits a WWW server CGI program to check the identity of an individual before returning a WWW page. SideCar listens for authentication requests from a web server. If a ticket is available (eg. if a person has already authenticated with KClient) SideCar simply returns the ticket. If no ticket is available, SideCar asks KClient to present the authentication dialog, and then sends the resulting ticket back to the requesting web server.

Back to Kerberos Authentication at Dartmouth

Last modified on 08/23/99 by MML
©1999 Trustees of Dartmouth College

OIT
Remote Access

Search OIT

Remote Home
DukeNet modem
ADSL Service
AT&T Internet Svc
Other ISPs
Proxy Server

Computers
Internet Access
OIT Help Desk
Search DUNK

Telephones
Cable TV & Video
Wireless

About OIT
OIT Site Index
OIT Home

Duke Home

Remote Access Options
Connecting from off-campus

Duke sponsored internet service options

DSL (digital subscriber line) from Verizon
This program offers high-speed data communications using phone lines, and is recommended and supported by the OIT Help Desk.

AT&T Internet service
This program offers you special rates for AT&T's dial-up Internet services.

DukeNet modem pool
The modem pool allows traveling students, faculty, and staff who have an acpub account to quickly check e-mail from off-campus locations. Because connection time is limited to 15 minutes, Duke recommends connecting through a commercial ISP for other online tasks. For more information on alternative ISPs see below.

Proxy server information
Accessing Duke sites when you use a commercial Internet provider. To access Duke-restricted resources such as Site-License software or some library resources when using an ISP, you may be required to use OIT's proxy service. View this web site for details on setting up your system.

Cable modem Internet service providers

RoadRunner (Time Warner)
A cable connection lets you access Internet service via a cable television jack.

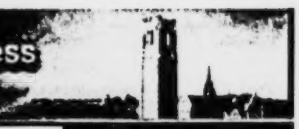
Alternative Internet service providers

Free, low-cost, or high-speed Internet service.
OIT provides a list of other Internet service providers. OIT does not endorse any of these services (except Verizon DSL) -- this is just a starting point to help you find the service that best suits your needs. If you need more help, call or stop by the OIT Help Desk, 101 North Bldg., 684-2200.

Questions? Send a message to help@oit.duke.edu.

UNIVERSITY OF FLORIDA
George A. Smathers Libraries

Guide To Remote Access
To Library Databases



Proxy Info | "Classic" LUIS | Networked CD-ROMS | Distance Learning | Having Problems?

U.F. Libraries

ALERT! While the UF Libraries' Catalog and a number of other resources available on the library web site are freely available to anyone connected to the Internet, **many databases and E- Journals available there are governed by licenses with publishers or other commercial vendors.** While generally anyone may use these resources within the UF Libraries, **access outside the Libraries from non-UF workstations is limited to current UF students, faculty, and staff,** and you must verify your current UF affiliation before being connected.

In preparation for verifying your current UF affiliation when connecting remotely, you should:

- **Activate the library number on your Gator 1 Card.** This 14-digit number beneath the barcode beginning with 200 will be required when dialing up any way besides using GatorLink, and may be needed from some UF workstations (if unable to connect directly). **In order for the number to work for remote access**, you must have used your card to check out a library book, or must have specifically asked for it to be activated at any UF Libraries' Circulation Desk. **Not sure if your current library number is activated?**
- **Obtain a GatorLink account.** This will enable you to dial-up to the UF for Internet services and access most library resources as if you were in the library.

Remote Access Options - Licensed Library Web Resources

From UF Workstations
(In campus offices, dorms, at IFAS Centers...)

Normally you should be able to access the UF Libraries' licensed Web resources as if you were in the library. NOTE: Occasionally a license limits access to workstations located in one or more UF Libraries.

If you find that you are unable to connect directly, it may be due to the way your local network access has been set up by your network administrator. Fortunately you still have two options:

- Set up your Web browser to use the **Library Proxy Connection** for access. This requires an activated library number.
- Use one of the "dial-up" access approaches described below for people not using a UF workstation.

From Home or Other Non-UF Workstation

Dial-Up to UF GatorLink

Dialing up to connect to the UF Network using a **GatorLink Account** enables you to access the Internet and all of the licensed library Web databases as if you were working in the library. While this will often be an excellent way to gain access to library resources, keep in mind the following limitations:

- If you are dialing long-distance, there will be telephone charges.
- Your GatorLink account includes a basic amount of connect time each month; then charges accrue. More...

Getting Set Up for Access Using GatorLink
You can register for your free Gatorlink account at the GatorLink web page or by going to the CSE building, Room E520. Telecommunication software is available on the UF software CD (which you can purchase from the Technology Hub) or by downloading from the UF Software site. Call (352) 392-HELP (UF Computing Help Desk) for more information and assistance in getting set up.

Phone Numbers for Dialing Up to GatorLink
955-0056 Settings: N-8-1 Baud Rate: 56kbps
Other Dial-Up Numbers (1-800 and ISDN/MPPP) NOTE: Surcharge for 800# use

Other Dial-Up Internet Service Provider (ISP)
(AOL, BellSouth, IBM ICE, ...)

The **library proxy server** is a special computer located on the UF campus that allows you to enter your library USERID (your 14-digit library number) and PASSWORD (UF) to verify your current UF affiliation. After verification, all your internet traffic passes through this computer (until you turn off access using the proxy). **This is the only way that you can dial up to access many resources (e.g. Lexis-Nexis Academic Universe, Web of Science...) if you are not dialing up to UF using GatorLink.** To learn how you can configure your specific Web browser, **connect to Library Proxy Connection Information.** When not needed for accessing library databases, you should turn off the proxy connection to maximize your response time using the Web.

> **Your ISP and the Library Proxy**
> Some Internet Service Providers (ISP) may intentionally block your browser's ability to use a proxy server, so you may wish to ask about this when signing up. **If you find that you are unable to access the library proxy through your ISP,** you may also set up Internet access using your **GatorLink** account (see above).

The following database services may normally be accessed without setting up your Web browser to go through the Library Proxy Connection. Instead, when trying to connect, you should simply be prompted to enter your 14 digit library number (no password).

		• WebLUIS Indexes *(20+ databases)* • UF Course Reserves (In WebLUIS) • FirstSearch *(60+ databases)* - Connects to Menu • Eureka *(15+ databases)* + RLG Archival Resources • Cambridge Scientific *(60+ databases)*
	Other Direct Connection *(Cable Modem, DSL, Ethernet...)*	If you are **not dialing up using a telephone modem, but are instead connecting directly to the Internet using a high-speed access option** like cable modem, DSL, or ethernet (e.g. from some Gainesville apartment complexes) your options should be the same as shown immediately above in the **"Other Dial-Up"** section. This is also the case if you are visiting another University to do research, etc. and are connecting to the Internet using their network.

U.F. Home

Copyright © 1999-2000 University of Florida George A. Smathers Libraries
P. O. Box 117001 Gainesville, FL 32611-7001
Acceptable Use, Copyright, and Disclaimer Statement
Send comments and/or questions about this site to
lib-webmaster@mail.uflib.ufl.edu
Last Updated October 2, 2001

UNIVERSITY OF FLORIDA
George A. Smathers Libraries

Guide to Remote Access
Using a Proxy Connection

U.F. Libraries

Setting Up Your Web Browser | Databases Available Using the Proxy

Why is a Proxy Connection Needed?
Many of the library databases and E-Journals available over the Internet are governed by licenses with publishers and other commercial vendors that require limiting access to current UF students, staff, or faculty (or to others who are using the resources within the Libraries). In order to enforce these access limits outside the Libraries, valid UF workstation addresses (IP numbers) are supplied to these vendors. When connecting from a UF workstation (whether in the library or not) -- or dialing up to connect to UF for Internet access using GatorLink -- the vendor recognizes that you should be allowed to use the resource without having to further verify your current UF affiliation.

UF Workstation	==========> Connection Allowed Automatically from "Known" UF Workstation	Database Provider

However, when you try to connect from an "unknown" workstation address IP number (when dialing up from home, etc. using a commercial Internet Service Provider) you are blocked from entry by the database provider. Although some UF Libraries' resources can be easily accessed by simply entering your "activated" 14 digit library number when prompted, access to others requires setting up your web browser to go through a Proxy Connection (a campus computer having an IP address that the database provider recognizes). After configuring your web browser with the Proxy Connection settings, you will be prompted to enter a USERID (your 14-digit library number) and a PASSWORD (**UF**) to prove your current UF affiliation each time you log on. Then you will appear to the database provider as if you are actually at a UF workstation.

"Unknown" Workstation	=====>	**UF Libraries' Proxy Connection** (Enter 14-digit library number to verify current UF affiliation)	=====>	Database Provider

Use the Proxy Connection Only When Needed
Once connected through the Proxy, **all** of your Internet activity will be routed through that workstation address (which the vendor recognizes as valid) until you turn off the proxy setting on your web browser. **You should connect using the UF Libraries' Proxy Connection ONLY when you want to use library databases. You should de-activate the use of the Proxy when you do not need it. Otherwise your browser's response time and/or ability to reach other desired web sites may be affected.** If you are unexpectedly asked for your 14 digit library number every time you load your browser, then the Proxy is probably still active and needs to be deactivated unless you intend to use the restricted library databases.

Warning! - Proxy Won't Always Work
Some Internet Service Providers (ISP) may intentionally block your browser's ability to use a proxy server. Should you have problems accessing databases using the UF Proxy Connection, please contact your ISP or local network support personnel. The Library can do nothing about that. If you are unable to connect through your ISP, you may also have to set up access using your GatorLink account. However, if you are not dialing up from a local number, this will involve long distance charges.

Library Web Services Available Using the UF Proxy Connection

You may use the Proxy for all library databases and E-Journals -- Databases available through links in the Database Locator, the Quick Links A-Z page, or the E-Journals page should have now been set up to allow access using the UF Proxy Connection. NOTE: Occasionally a license limits access to workstations located in one or more UF Libraries.

The proxy is not always required -- When you wish to connect to the following databases, you do NOT need to use the Proxy Connection. For these resources you should be prompted to simply enter your 14-digit library number (no password) at the time you enter each database service using any Internet Service Provider (ISP). Although you may connect to these resources using the library proxy as well, routing these transactions in this way (through an intermediate computer) may result in unnecessarily slow response time.

- **WebLUIS Indexes** (20+ databases)
- **UF Course Reserve**
- **FirstSearch WITHOUT the Proxy** (60 + Databases) | FirstSearch WITH the Proxy
- **Eureka** (20 databases) + RLG Archival Resources (Separate Eureka Connection)
- **Cambridge Scientific Abstracts** (60+ databases)
- **Uncover**

If you can't connect to a database, please report the problem to lib-webmaster@web.uflib.ufl.edu

UF Proxy Setup Instructions

Listed below are links to the Proxy Connection setup instructions for the minimum browser versions recommended. Instructions for some older versions may still be available, but we recommend upgrading your browser.

Netscape 4

Internet Explorer 5

If you are dialing up using a telephone modem -- or have a DSL connection
If you have a direct connection to the Internet (e.g. using a cable modem, ethernet service, or in a campus office.)

Internet Explorer 4

AOL users: Because AOL's web browser does not allow you to modify your proxy settings, you must download a different browser that will allow this setup.

U.F. Home

Copyright © 1999-2001 University of Florida George A. Smathers Libraries
P. O. Box 117001 Gainesville, FL 32611-7001
Acceptable Use, Copyright, and Disclaimer Statement
Send comments and/or questions about this site to
lib-webmaster@mail.uflib.ufl.edu
Last Updated September 7, 2001

Off Campus Access: A Guide to the McMaster Proxy Service

UNIVERSITY HOME PAGE | SEARCH TOOLS | COMMENTS | NEWS

Purpose of the McMaster Web Proxy Service
How to Set Up Proxy Service
Help

Purpose of the McMaster Web Proxy Service

- Provides access to library resources (such as e-journals) which are restricted for use by the McMaster community
- For current McMaster faculty, staff and students using commercial internet service providers (such as Interlynx)
- McMaster Modem pool users do not need this service

How To Set Up Proxy Service

Step 1 - Apply for a Proxy ID (User name and password)

Undergraduate, graduate students and residents	◆ Apply through MUGSI
McMaster Faculty and Staff (Roll 1)	◆ Visit the CIS Main Office (ABB-132) or ◆ E-mail carmela@mcmaster.ca.
Staff (Roll 3)	◆ Complete application form available at CIS (ABB-132). *Note:* Form must be accompanied by a sponsor letter/email (to carmela@mcmaster.ca) from a Roll 1 employee.
McMaster Appointees and Affiliates: sabbatical visitors, visiting scholars or researchers	◆ Complete application form available at CIS (ABB-132). *Note:* Form must be accompanied by a sponsor letter/email (to carmela@mcmaster.ca) from a Roll 1 employee
Faculty of Health Sciences Appointees and Affiliates	◆ Complete application form and return with a sponsorship letter to: Morag Horsman, CSU, HSC-2D9, McMaster University

Step 2

Undergraduate and Graduate Students, and Residents – Wait 24 hours for your account to be activated

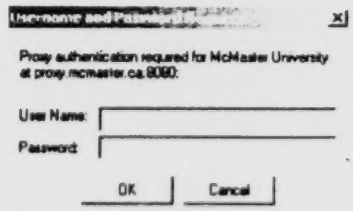
Faculty, Staff (Roll 1 and 3), Appointees and Affiliates – Wait for notification that your account has been activated.

Step 3 - Configure your browser

Netscape 4.5, 4.7 or 6.2
Netscape 6.0
Internet Explorer 4.0
Internet Explorer 5 & 6 (all versions) - Cable Modem Connection
Internet Explorer 5 & 6 (all versions) - Dial-Up Connection

Step 4 - Check to make sure everything is set up correctly

- If you click on any of our restricted resources, a box as shown below should appear



- If you don't get this box, then go back to step 3 and make sure you've done everything correctly
- Click Here To Test Your Proxy Setting

Help

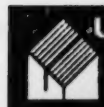
Contact CIS Help Line

Phone: (905) 525-9140, Ext. 24357 8:30am - 4:30pm
Email: helpline@mycmail.mcmaster.ca

Updated December 10, 2001

Electronic Resources

BEST COPY AVAILABLE



University of Manitoba Libraries

Welcome to UML | Contact Us | Site Index | How to use this site | Search

Help Pages

Using the Proxy Server to Access Restricted Databases and Web Resources

The Libraries subscribes to a wide range of useful databases and web resources on behalf of current University of Manitoba faculty, staff, and students. To comply with our licensing agreements, access to most of these resources is limited to computers connected to the UM campus network (either directly or through the UM Modem Pool).

To use these resources from computers which are not connected to the UM campus network, you must configure your Web browser to access them through the UML Proxy Server. The Proxy Server asks you to enter your Library ID Number and PIN, and then connects to the restricted resource on your behalf -- allowing you the same access privileges as computers located on campus.

Who *should* use the Proxy Server?

- Eligible users who connect to the Internet from a computer that is **not on the UM campus network**. This includes:
  - Computers with dial-up (modem) connections through Escape, MTS Sympatico, or any other Internet Service Provider other than the UM Modem Pool.
  - Computers with cable modem or ADSL connections.
  - Computers at any off-campus location with direct (LAN) connections to the Internet.
- Eligible users who experience "Access Denied," "Not Subscribed," or similar error messages when trying to access a restricted library resource or database.

Who *shouldn't* use the Proxy Server?

If you are using a computer connected to the UM campus network (directly or through the UM Modem Pool) **you should not use the Proxy Server**. You should be able to access restricted library resources directly. Using the Proxy Server will only slow your connection, and force you to log in unnecessarily.

How do I configure my Web browser to use the Proxy Server?

Configuring your Web browser to use the Proxy Server is simple, but each one is a little different. Select your browser from the list below to see specific setup instructions.

- Netscape Navigator or Communicator (version 4.x)
- Netscape Navigator (versions 2.x or 3.x)
- Microsoft Internet Explorer (version 5.x)

BEST COPY AVAILABLE

- Microsoft Internet Explorer (version 4.x)

Microsoft Internet Explorer 6 and Netscape Navigator 6 users

While the proxy configuration files have not been tested with Microsoft Internet Explorer 6 or Netscape Navigator 6, we have some patrons who are using these browser versions successfully. You are welcome to try to configure your browser.

For Microsoft Internet Explorer 6 use the Microsoft Internet Explorer 5.x instructions.

For Netscape Navigator 6 use the Netscape Navigator or Communicator (version 4.x) instructions.

How do I determine my user name and password (Library ID Number and PIN)?

When the Proxy Server asks you to enter a user name and password, it expects you to enter your Library ID Number as the user name, and your Library PIN as the password. See Determining Your User Name and Password if you aren't sure what your Library ID Number and PIN are.

Note: For security reasons, the Proxy Server **will not accept the "default" PIN** as a valid password, even if it is correct. You *must* change your PIN at least once before you can use the Proxy Server. To learn how to change your PIN, please refer to the instructions at the end of the Determining Your User Name and Password page.

The University of Manitoba Libraries
Winnipeg, MB, Canada R3T 2N2, (204) 474-9881
Questions or Comments? Email the WWW Developer.
© 1996-2001, University of Manitoba Libraries

Last Updated: 16 November 2001

MIT Information Systems

Obtaining MIT Certificates: Quick Guide

On this page: Introduction | What You Need Before You Start | MIT CA Certificate | Get Your MIT Personal Certificate | Security Settings

Introduction

From this page you can obtain Web certificates that will let you access MIT's secure Web services. You will need to get a set of MIT certificates for each computer you use.

For more detailed information, especially if this is your first time to get MIT certificates, go to Obtaining Certificates for Accessing Secure Web Services at MIT. If your situation matches any in the list below, follow that link to more information.

- Your personal certificate has expired.
- You wish to check the expiration date on your personal certificate.
- You need information on setting certificate security preferences.
- You are taking over a computer containing certificates for a previous user.
- You share a Macintosh or Windows computer.
- You are getting certificates on Athena.

What You Need Before You Start

- Your valid MIT ID number.
- Your Kerberos username and password (same as for Athena, MITnet, or Eudora e-mail).
- Netscape 4.6 or up through Netscape Navigator 4.78 , the current supported and recommended browser at MIT, installed on each computer on which you are getting certificates. The MIT installation of 4.78 includes the MIT CA certificate (see below). Note: Instructions for configuring certificates only for Netscape are given in this guide.

  Athena users may get and use MIT Web certificates with Lynx, the text-based browser. Windows users may obtain certificates for Internet Explorer 5.5.

If you do not have any or all of the above, go to Prerequisites to Getting MIT Web Certificates for details.

The MIT CA Certificate*

You must have the MIT Certification Authority (MIT CA)* certificate before you can get a personal certificate. If unsure about having one, see Check for the MIT CA.

*Previously known as the "site" certificate.

Get Your MIT Personal Certificate

Your MIT personal certificate authenticates you to the secure MIT Web server. It proves to the secure server that you are who you claim to be. The process for getting a personal certificate takes you through four screens of information and instructions. Details.

Note: If your personal certificate has expired, see When Personal Certificates Expire. To check the expiration date on your personal certificate, see Determine When Your Personal Certificates Expire.

Security Settings

Netscape lets you set certain certificate-related security preferences, either during the process of getting a site and personal certificate, or through the Security settings panels. For details, go to Recommended MIT Certificate Security Preferences.

Comments about these pages
Last modified: December 4, 2001

LIBRARIES
THE UNIVERSITY OF NORTH CAROLINA AT CHAPEL HILL

OFF-CAMPUS ACCESS VIA PROXY SERVER

Supported Browsers

Netscape:

Communicator 3.x

Communicator 4.x

Communicator 4.5 or higher for Macintosh computers

MS Internet Explorer:

Internet Explorer 3.02

Internet Explorer 4.x

Internet Explorer 5.x (Dial-up Connection)

Internet Explorer 5.x (Cable Modems/DSL/LAN)

Internet Explorer 4.1 for Macintosh computers

AOL, CompuServe, & MSN:

Special Instructions for AOL, CompuServe, & MSN Users

WebTV:

Instructions for WebTV Users

Help:

FAQ: Frequently Asked Questions About Remote Access

TROUBLESHOOTING

Information and Instructions

Many of the electronic resources provided through UNC-Chapel Hill Libraries are licensed to be used only by current UNC-CH students, faculty and staff or UNC-CH affiliated AHEC faculty, staff, preceptors, and residents. To comply with these license agreements, access is often restricted to the Internet Protocol (IP) address range associated with the Chapel Hill campus. For students, faculty and staff who access the internet through third-party internet service providers (ISPs) such as Bellsouth.net, Mindspring/Earthlink, AOL, and IBM, this presents a problem. The IP address owned by the ISP will not be recognized as a valid UNC-CH address and access to the licensed resource will be denied. To remedy this situation, UNC-CH Libraries have installed a proxy server. The proxy server has a valid UNC-CH IP address. If the user's web-browser has been configured to use the proxy server, access is available for almost all of the resources.

What is a Proxy Server?

A proxy server is a combination of software and hardware which acts as an intermediary between a set of users and the Internet. It allows authorized users to access almost all restricted electronic resources available through the UNC-CH library web pages from home or on the road. Users must configure their browser with the address of the proxy server to enable this option.

What do I need to do?

In order to be able to access restricted services from the UNC-Chapel Hill Libraries, you must configure your browser.

Show me configuration instructions for my browser

NOTE:
If you choose to use MSIE 5.x, we recommend using MSIE5.5sp1 as the preferred release. You may download this version from http://www.microsoft.com/windows/IE/.
You may download Netscape 4.x from http://shareware.unc.edu/index.html.

Test Browser Functionality Check Functionality of my browser

The above link checks your browser for cookie acceptance and JavaScript compatibility. It can assist in diagnosing basic setup problems.

Your browser must allow cookies to complete the validation process. More information on cookies from Netscape and Microsoft.

Remote Access Requirements:

- Netscape Communicator/Navigator 3.x or higher, or Microsoft Internet Explorer 3.02 or higher.
  (Do not download versions of Netscape 6.x or Internet Explorer 6.x. Bugs have been identified in these versions and a patch to correct the problems is not yet available from the vendors.)
- Java and JavaScript enabled in your browser, and it must be set to accept cookies. These are the default settings in your browser. If you have disabled them, you must change your configuration before attempting to connect to a research database.
- Your browser configured to use the library's proxy server. You only need to configure your browser once.
  If your Internet access is through a networked computer located on the UNC-CH campus, you do ***not*** *need to reconfigure your browser.*

STEP 1: Determine which Internet browser you are using:

- Open your Browser (Netscape, Explorer, etc.)
- Click "Help" on the browser menu on the top of the screen
- Click "About (name of browser)"
- A window will open which provides the version of the browser (4.0, etc.)
- Proceed to Step 2, "Select your browser type for configuration instructions"

STEP 2: Click on the appropriate browser link to the left to display the reconfiguration instructions.
NOTE: BE SURE TO PRINT OUT THESE INSTRUCTIONS BEFORE YOU BEGIN RECONFIGURING YOUR BROWSER SETTINGS!!

Authentication:

When selecting a restricted resource, you will be prompted to authenticate yourself with either your PID or your AHEC Digital Library username and password. **You will only need to enter your PID or AHEC Digital Library account at the first restricted resource to be authorized for the entire session of the browser.**

It is not necessary to return your browser to its original settings prior to visiting non-UNC-CH Library resources. The autoconfiguration settings will determine the correct routing without any intervention on your part. However, if you use another proxy server in addition to the UNC-CH proxy server, you will need to change your proxy settings in order to use the different proxy server. Please consult the configuration instructions for your browser to relocate the UNC-CH proxy settings so that you can remove them.

UNC-CH faculty, staff and students: if you have questions regarding the PID system, please consult the University's information regarding the establishment of these numbers. UNC-CH Person ID Project

AHEC staff, faculty, preceptors and residents: if you have questions regarding your AHEC Digital Library username and password or if you do not yet have an account, please see information on the AHEC Digital Library web site at: http://library.ncahec.net/, including the Documentation for new users. NOTE: It is no longer necessary to use or request a BID to login to restricted resources through the UNC-CH Proxy Server.

The content of this page was adapted from Central Michigan University's Off-Campus Library Services web site.

Home | Online catalogs | Resources | Library Information | Services | DAS | UNC Home

If you have any questions, problem reports, or comments please contact the UNC-CH Proxy Server Team via email. You may also call Library Systems (919) 962-1288 Monday-Friday 8AM-5PM, or the Davis Library Reference Desk (919) 962-1356.
URL: http://proxy.lib.unc.edu/
This page was last updated Tuesday September 14, 2001.

SERVICES

University of Oregon Library System

Off-Campus Access to Library Databases

The UO Library provides access to a number of databases and electronic resources for the campus community. Eligibility for access to a specific resource is based upon the terms of the licensing agreement signed by the library. Most electronic resources recognize authorized users based on campus IP (Internet) address. UO students, faculty and staff who use the Computing Center's modem pool have full access to electronic resources offered by the library.

Students, faculty and staff who use a non-UO Internet Service Provider (ISP) may now gain access to the library's electronic resources by using the library's proxy server. The proxy server, which has a UO IP address, acts as an intermediary between an off-campus computer and a database. To use the proxy server, the settings or preferences in a Web browser need to be modified. Students and faculty using the proxy server will be prompted for their name and ID when they select a link with restricted access. After being authenticated as a UO patron, the requested database allows the connection to be made as if the request were coming from an on-campus computer.

- Modify browser preferences
- PC instructions
- Mac instructions
- Security Alert
- ID & password instructions
- AOL users
- Off-Campus Access FAQ
- Need help?

BEST COPY AVAILABLE

University of Washington

Computing and Networking | Search | Directories | Reference Tools

About UW NetIDs

Get Your UW NetID and Password

Affiliate Services

Use your UW NetID to:
Sign up for basic computing services

Reset a forgotten password

Change your UW NetID password

Manage your computing services

Open MyUW (your personal Web portal)

Learn more about UW NetID by reading:
Knowing the rules

Choosing a good UW NetID and password

List of computing services and links to documentation

Your UW NetID (with password) is your **personal identification** for using UW online resources. A UW NetID is required of everyone associated with the University of Washington who plans on using online central administrative and computing programs. These include Web interfaces used to:

- Check your personal information (student grades and schedules, employee payroll records and benefits files).
- Access secure applications required for university administrative work (financial, payroll, and student databases).
- Set up UW email accounts with forwarding options, along with other computer services (dial-in modems, lab access, research computing, and a MyUW page to customize as your personal portal to campus information).

Get Your UW NetID and Password now so you will have it when you need it.

Why is a UW NetID necessary?

Your UW NetID verifies who you are when you use the many UW network services. Such verification ensures the privacy of your personal information and restricts the use of resources to those for whom they are intended. To make access to such services more secure and consistent, the UW is consolidating the identifications you need to just one: the UW NetID.

To get help or make comments about the information on this page, use the **Send a Question to C&C** Web site.

UNIVERSITY OF WASHINGTON
Computing & Communications
help@cac.washington.edu
Modified August 2, 2001

Connecting to the Libraries

If you have a current UW Husky card, know your library PIN, and are trying to access our online resources from off-campus you can connect directly to the Proxy Server Wizard

If you are no longer affiliated with the University, you should remove proxy service settings from your browser.

FAQs about connecting to the Libraries' online resources

- How do I connect my computer to the Internet?
- I tried to use one of the libraries' databases and it asked me to log in. I entered a user name and password, but it didn't work. What do I do now?
- What do I need to use the proxy server or the proxy server wizard?
- What are UW-restricted databases and who can use them?
- Are there any known bugs or problems that might affect my connection to the Libraries' online resources?
- How can I get to electronic reserve materials?

How do I connect my computer to the Internet?

You can use the UW Internet Connectivity Kit (UWICK) or you can contract with a third-party Internet Service Provider (ISP) to connect to the Internet. Computing and Communications maintains a web page on Internet connectivity that provides details about each of these options.

If you use the UWICK for Internet access you should have no problems accessing the Libraries' online resources. If you use an ISP such as Earthlink or @Home you will need to configure your browser to use the proxy server.

back to the top

I tried to use one of the libraries' databases and it asked me to log in. I entered a user name and password, but it didn't work. What do I do now?

If you got a page from a database vendor such as Proquest, Gale, or WebSPIRS that asked for a username and password, you will need to set up your browser to use the proxy server.

Many services offered by the UW Libraries are available only to current UW students, faculty, and staff. At present, most of these licensing restrictions are enforced based on the Internet Protocol (IP) address of the computer that you are using to access the Internet. If you are accessing the Internet from an off-campus computer, then your IP address would be assigned to you by your Internet Service Provider.

A proxy service allows you to authenticate with the UW Libraries using your UW Libraries barcode and PIN, in order to gain access to UW-restricted services from non-UW IP addresses. A proxy server wizard to help you configure your browser is available at http://www.lib.washington.edu/asp/browser/proxy.asp

When using the proxy server, the 14-digit barcode (it starts with 29352) on the back of your Husky Card is your username and your library PIN is your password. Once you have correctly configured your browser to use the proxy server, you need to close your browser window and then open a new one. The first time that you try to use a UW-restricted database during an Internet session, you will be prompted for your username and password. After that you will not have to enter this information again during that session.

Back to the top

What do I need to use the proxy server or the proxy server wizard?

1. A current UW Husky Card
   - On the back of the card you will see a 14-digit number that begins with 29352. This number is your username when using the proxy server and proxy server wizard.
2. Your Husky Card needs to be in the Libraries' circulation system. This happens when you:
   - Use the card to check out something from a library
   - Bring your card to a circulation desk and ask that it be linked in the system
   - Use our online form to have it linked for you. This can take up to 2 days so if you need immediate access to the restricted resources you will need to bring your card to the library and have it linked in person. We cannot link barcodes over the phone.
3. Your library PIN
   - If you don't have a PIN, you can set one up online by following the instructions on the View Your Record page.
   - More information about PIN management can be found at http://www.lib.washington.edu/services/borrow/pin.html

Back to the top

What are UW-restricted databases and who can use them?

These are databases that are contractually restricted to current University of Washington faculty, students, and staff, or to persons physically present in the University Libraries. In most cases, this restriction is enforced by the vendor with an IP address check; only requests originating from computers on the University of Washington network (including the dialup modem pool) are considered valid unless the proxy server is used.

Back to the top

Are there any known bugs or problems that might affect my connection to the libraries' online resources?

Check our Known Issues and Bugs page for information about software conflicts.

Back to the top

How can I get to electronic reserve materials?

Reserve material, including electronic reserves, can be found in the UW Libraries online catalog. You can search the course reserves either by course (i.e. GEOLOGY 101) or professor's last name (i.e. Smith). Listings in the online catalog are in alphabetical order.

Electronic reserves are indicated by an item named "ELECTRONIC READINGS FOR ____." Click on that item to get to a link that says "Connect to this title online". Click on that link, then enter your UW NetID to bring up a list of electronic files for the class.

libquest@u.washington.edu
Last modified: Friday August 03 2001

UW Home | Gateway Home | Gateway Index | Search

© 1999-2001 University of Washington

Washington University Libraries

Home • Catalogs • Databases • Full-text • Reference • Web Sites • Research Help

Proxy Setup Instructions

If you wish to access restricted Internet resources (that is, those databases and electronic journals which are restricted by license or contract to current WU students, faculty, and staff) when using a non-Washington University Internet Service Provid er, follow the instructions below. Such access works via a proxy service established by the WU Libraries. *(If you're using your WUStL email account to make a PPP connection to the campus network, you don't need to use the proxy server. See access to restricted resources for more information.)*

You must set up your web browser for proxy service. This is a one-time setup; once you have configured your browser, you don't have to do it again - unless you get a new browser.

FIRST, follow the instructions in the table below for your browser (scroll down this page to see instructions for Netscape, Internet Explorer, and for AOL users). If you have problems, please contact your Internet Service Provider or webmaster@library.wustl.edu.

THEN, once you have configured your browser:

1. Access the WU Libraries' homepage, at http://library.wustl.edu/.
2. Click on the resource you want to connect to.
3. The *first* time you do this each time you open your browser, you will be challenged for your name, your WU ID number, and your PIN. (If you do not have a PIN, go to View Your Library Record/Create Library PIN to choose one.)
4. Fill in the requested information, and click on the Submit button.
5. You will be connected to the resource. You should not be challenged again for your name, ID, and PIN - until you close your browser, or unless you leave your connection idle for 10 minutes. (Your browser settings may affect timeouts and the caching of access permissions.)

Please note: *Not all databases and electronic journals are accessible via the proxy server.* In some cases, this is due to licensing restrictions by the database vendor or journal publisher. See this list of the resources that are available! If there is a resource you wish to use which is denying you access, please send a message to webmaster@library.wustl.edu, indicating the name of the resource. We'll let you know if that resource can be made acessible via the proxy service or not.

NOTE:

- Problems have been reported when trying to use the proxy server with Netscape 6. The problem has been reported to the software vendor, but the only solution at this point is to keep an older version of either Netscape (or IE) to use with the proxy server. [11/30/00]
- A serious problem with Internet Explorer 5.0 and proxy autoconfiguration has been discovered. [12/16/99] Internet Explorer 5.01 *is* apparently working with the proxy server. [1/19/00]

BEST COPY AVAILABLE

Netscape Version 3	Netscape Version 4
1. select **Options** 2. select **Network Preferences** 3. select the **Proxies** tab 4. enter in the **Configuration Location (URL):** http://spokane.wustl.edu:8080/proxy.pac 5. click **Reload** and **OK**	1. select **Edit** 2. select **Preferences** 3. click on the '+' to the left of the **Advanced** option 4. click on **Proxies** 5. click on the **Automatic proxy configuration** button 6. enter in the **Configuration Location (URL):** http://spokane.wustl.edu:8080/proxy.pac 7. click **Reload** and **OK**

MS Internet Explorer Version 3.02	MS Internet Explorer Version 4 (SP1)
1. select **View** 2. select **Options** 3. select the **Advanced** tab 4. at the bottom of the **Advanced** page, click on the **Automatic Configuration** button 5. enter in the **URL:** http://spokane.wustl.edu:8080/proxy.pac 6. click on **Refresh** then click on **OK** in the popup box 7. click on **Apply** then **OK** on the **Options** menu	1. select **View** 2. select **Internet Options** 3. select the **Connection** tab 4. in the **Automatic configuration** box click on **Configure** 5. enter this **URL:** http://spokane.wustl.edu:8080/proxy.pac 6. click on **Refresh** 7. click on **OK** then **OK** again on the **Internet Options** menu

MS Internet Explorer Version 5	
Dial-up Modem Connection	Local Area Network (LAN) Connection
1. Select: **Tools** 2. Select: **Internet Options...** 3. Select: **Connections** 4. In the **Dial-up settings** box find the icon with the name of your dial-up service. Click on the icon once to highlight it. 5. Select: **Settings...** 6. Check the box next to: **"Automatically detect settings"** 7. Check the box next to: **"Use automatic configuration script"** 8. enter this **Address** http://spokane.wustl.edu:8080/proxy.pac 9. click on **OK** 10. click on **OK** on the **Internet Options** menu	1. Select: **Tools** 2. Select: **Internet Options...** 3. Select: **Connections** 4. Select: **LAN Settings** 5. Check the box next to: **"Use automatic configuration script"** 6. enter this **Address** http://spokane.wustl.edu:8080/proxy.pac 7. click on **OK** 8. click on **OK** on the **Internet Options** menu

MS Internet Explorer Version 6
Detailed instructions not yet available. However, it has been reported that proxy settings should be put in Dial-up Settings, Settings button, Use Automatic Configuration script. Same address as above (http://spokane.wustl.edu:8080/proxy.pac).

Notes for AOL Users
1. To install Netscape Navigator for AOL: 2. Keyword: **netscape** 3. click on **Click Here!** 4. click on **Download Netscape** 5. Follow the prompts to load and install Netscape Navigator 6. Follow the steps listed above for setting up Netscape Version 4

© 1993-2001 Washington University, St. Louis, Missouri, USA

Connect from Home

TUG Proxy Service:
Remote Access to Restricted Resources

Who Can Use This Service?
How to Connect to the Proxy
1. Register with the TUG Libraries System
2. Designate the Proxy Machine in Your Browser
3. Login
4. Special Considerations
How to Get Help

Who Can Use This Service?

This service provides off-campus access to resources and services available only to **current students, faculty, and staff** of the University of Guelph, the University of Waterloo and/or Wilfrid Laurier University.

The restriction to use a database or service is imposed by the database provider or the site licence, or simply because of the nature of the service. These resources are accessible only from machines on campus (defined by IP domains: uwaterloo.ca, uoguelph.ca and wlu.ca). **If you use the University's modem pool to connect to the Internet from home, your computer is considered to be on campus, and you do not need to use the proxy service.** If you use a third party Internet service provider, you may log into the proxy server. It serves as a proxy machine between your off-campus computer and the restricted resources, and your request through the proxy will be treated as one originating on campus.

How to Connect to the Proxy

1. Register with the TUG Libraries System

Before you can use the proxy, you must have registered with TRELLIS, the automated library system connecting the library collections of the TriUniversity Group of Libraries. Registered users are students, faculty or staff who hold a current university ID card that has been validated (or activated) for use by the Library. If you have not validated (or activated) your card, you may do so in person at the Circulation Desk in the Library, or by **self-registration**. Distance education students may also register by phone or e-mail (see UG, UW, and WLU information pages).

The authentication database of the proxy server is updated with information in TRELLIS by an overnight process. Therefore, you can only start using the proxy the day following validation of your card, although you are able to borrow library material and place requests in TRELLIS immediately.

2. Designate the Proxy Machine in Your Browser

You need to **configure your browser** to designate the proxy. Please see instructions to configure some versions of **Internet Explorer** and **Netscape**.

Some resource providers use 'cookies'. If you are set up to use the proxy server and still encounter a login screen from a resource provider (e.g., ABI/INFORM), it may be that 'cookies' are disabled. **Make sure that "cookies" are enabled in your browser.**

Enter one of the following URLs in your **Proxy designation**:

- University of Waterloo registered users:
  http://www.tug-libraries.on.ca/proxy/uwproxy.pac
- University of Guelph registered users:
  http://www.tug-libraries.on.ca/proxy/ugproxy.pac
- Wilfrid Laurier University registered users:
  http://www.tug-libraries.on.ca/proxy/wluproxy.pac

Use of the wrong .pac file will not allow you to access the restricted resources of the other TUG Libraries. Authentication is based on your registered University affiliation.

If your machine has firewall protection, as some company or public machines do, the Web browser may have already had a designated proxy; you will not be able to access the TUG proxy service. You may discuss the problem with your systems administrator.

The browser may seem to be slower when working with the proxy, since the requests are sent to the resource providers through the proxy server.

3. Login

For each session you use the Internet browser to connect to the Library, you will be asked to login with the proxy only once, when you first start requesting a restricted resource or service. If you have subsequent requests of these resources or services in the same session, you do not need to login again.

The login process requires that you enter:

- **User Name**: Use the **bar code number** on your library card
  (no space in-between numbers)
- **Password**: Use your **last name** (lower case)

Warning: If you sign onto the proxy machine from a shared or public computer on which you are able to designate the proxy, you should close the Web browser after you finish, to prevent non-legitimate use of these resources or services in your name.

4. Special Considerations

AOL subscribers:

- Dial up and login to AOL as usual.
- Minimize the browser used to connect to AOL.
- Configure Netscape for the Library Proxy Service

Netscape:

- Netscape is free and is available at the Netscape web site. Netscape Communicator 4.78 is proven to be easy to configure for use with the Proxy Service.

How to Get Help

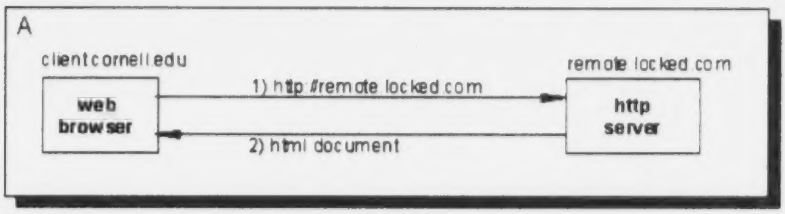
If you need any additional information, please contact the Information Desk in the Library. If you encounter any problem using the TUG Proxy Service, fill out the **Problem Report** form, and we will try to contact you within one working day.

Last Updated: 2000.11.10

Technical Specifications

How the Proxy Web Server Works

Currently web browsers connect directly to the remote vendors' sites, which are site-locked to allow access only from Cornell IP addresses.

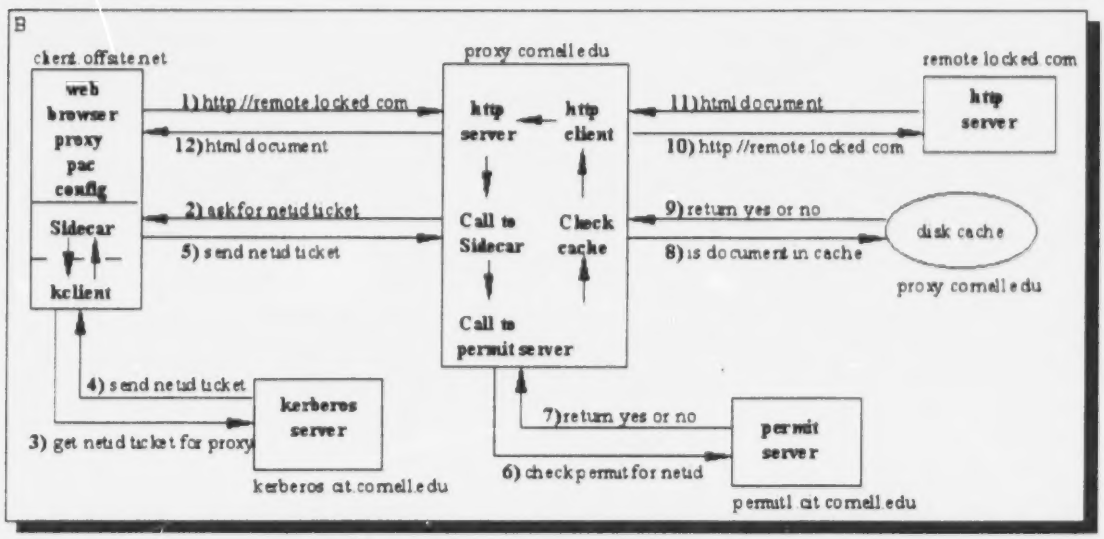


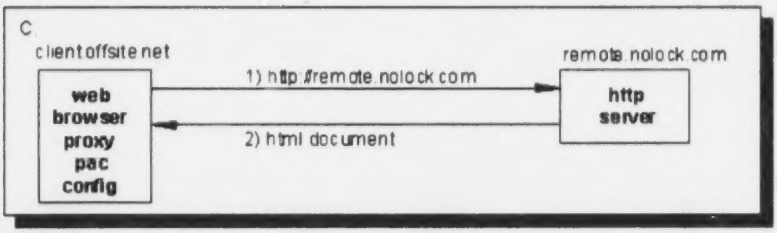
Using automatic proxy configuration and a JavaScript file called a proxy auto-config (or *pac*) file, we can configure off-site browsers to access the locked sites through a proxy server but contact other sites directly.

Sample pac file:

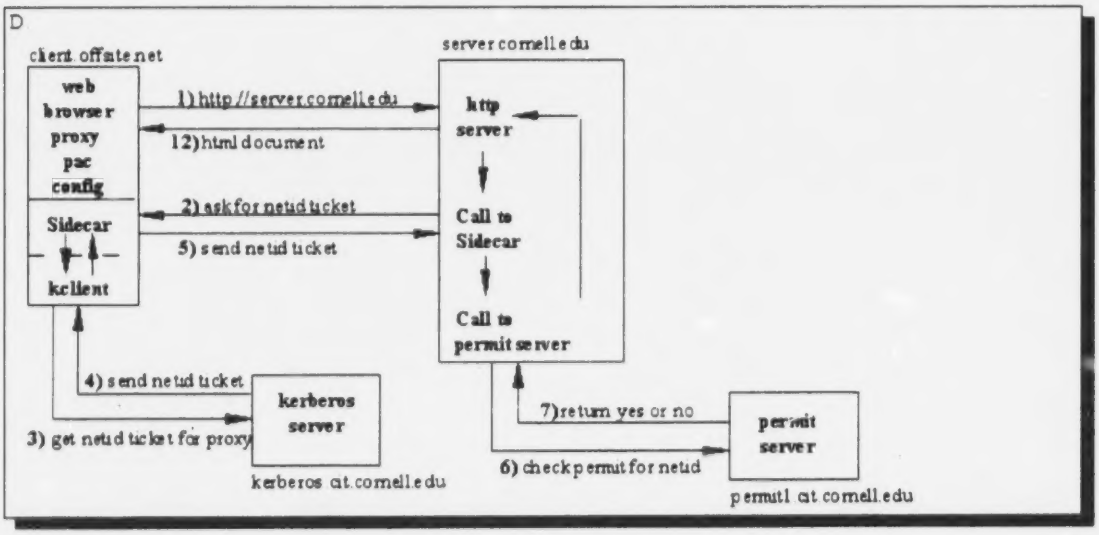
```
function FindProxyForURL(url,host)
{
   if (localHostOrDomainIs(host,"remote.locked.com"))
      return "PROXY proxy.cit.cornell.edu";
   else
      return "DIRECT";
}
```

With this pac file, transactions to locked sites go through the proxy server (Figure B) but other transactions use a direct connection (Figure C).





This same pac file works properly with on-campus web servers that use SideCar to authenticate their transactions. It sends the transaction directly to the campus server instead of through the proxy server (Figure D).



For more information, see:

- How Does Proxying Work? from the University of Pennsylvania Library
- What is Automatic Proxy Configuration (APC)? from the University of Pennsylvania Library

Introduction | Netscape | Internet Explorer | Technical Info

Computing at Cornell ➡ CIT Services ➡ Kerberos and SideCar ➡ Proxy Web Server

Last modified: October 19, 2000
Need help? Please use the Library Gateway's Technical Problem Report Form
Comments about this web page: cit_pubs@cornell.edu

BEST COPY AVAILABLE

UNIVERSITÉ LAVAL

Serveur Mandataire
Version 1.0

Détails techniques

Guide général

Table des matières

Fonctionnement 1

Schéma 1

Définition des paramètres 2

Sécurité 3

Les utilisateurs authentifiés 3

Les ressources disponibles par le serveur Mandataire 3

Le fichier LOG 5

Exception 5

L'interface utilisateur 6

Le code source du script proxy.pl, lignes à lignes 6

Statistiques 14

Table des matières 15

Serveur Mandataire

Techniques utilisées lors de la programmation

Fonctionnement

Un programme PERL, proxy.pl, se trouve au cœur du serveur Mandataire de la Bibliothèque de l'Université Laval. Ce programme, de fabrication maison, permet, à l'heure actuelle, une navigation passablement sans accroc sur une majorité de sites Web. Mais avec la constante évolution des technologies de diffusion de l'information sur le Web, il va sans dire que le programme devra, dans l'avenir, être adapté pour faire face à la musique. Cela signifie donc qu'une veille technologique devra être faite et qu'une certaine expertise en programmation CGI en PERL devra être maintenue afin de conserver un serveur Mandataire fiable.

Afin de répondre plus efficacement à ce besoin, ce manuel contient tous les détails techniques qu'il faut connaître au sujet du serveur Mandataire ainsi que des commentaires et des trucs utiles au programmeur qui aura la tâche de garder le serveur à jour.

Schéma

Le serveur Mandataire se veut un intermédiaire entre l'ordinateur du client et les serveurs Web. Il effectue la requête HTTP que le client lui envoie et lui retourne la réponse du serveur. On ne peut pas se servir du serveur Mandataire sans appeler le script proxy.pl. Quand le client a appelé le script pour la première fois, on dit qu'il est en « mode proxy », c'est-à-dire que le serveur Mandataire prend maintenant le contrôle de toutes les requêtes que le client effectuera. Il faut s'authentifier auprès du service Portail pour que le navigateur client puisse appeler le script proxy.pl une première fois. Après identification à l'aide du numéro de dossier (code zébré) et du NIP, Portail effectue la première requête au serveur Mandataire en spécifiant qu'il faut initialiser la session de travail. Le serveur Mandataire retourne alors un fichier HTML qui définit deux cadres. Le premier cadre est une sorte de bandeau qui contient des boutons de navigation et qui fait savoir au client qu'il vient de commencer la navigation en « mode proxy ». Le second cadre est la fenêtre de navigation principale, elle contient le résultat de la requête que le client a fait avant d'être amené au service Portail.

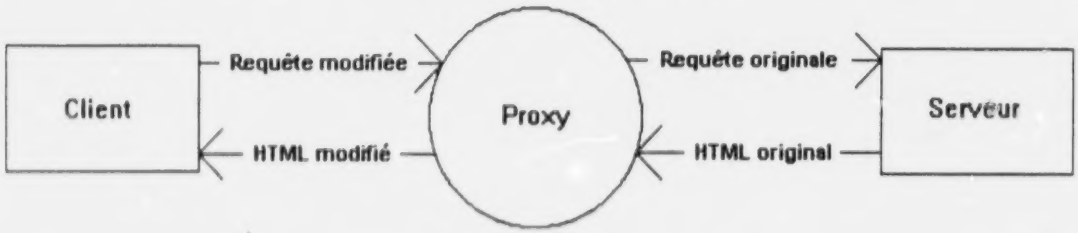
Comme le serveur Mandataire n'est pas un serveur « canal », c'est à dire qu'il n'exécutera pas automatiquement toutes les requêtes du client (exemple : MS Proxy 2.0 est un serveur « canal », une fois le numéro IP du serveur configuré dans les options du navigateur client, il se chargera automatiquement de toutes les requêtes), il a fallu mettre au point une façon de garder le client en « mode proxy ». C'est le cœur du système.

La méthode envisagée avait déjà été mise au point par des spécialistes du langage PERL. Le serveur Mandataire a donc été bâti à partir d'un programme existant. Cette méthode est assez simple : changer tous les liens (URL) du fichier HTML contenu dans la réponse du serveur afin qu'ils pointent vers le serveur Mandataire lui-même (présentement, http://proxy.bibl.ulaval.ca/cgi-bin/proxy.pl) au lieu de pointer vers le

document original. Pour que le serveur Mandataire sache quel était le document original et puisse aller le chercher pour le client, on lui greffe en paramètre au nouveau lien l'URL original rendu absolu. Si ce document est, par exemple, http://www.bibl.ulaval.ca/ Le nouveau lien devient alors :

```
http://proxy.bibl.ulaval.ca/cgi-
bin/proxy.pl?adresse=http://www.bibl.ulaval.ca/
```

On a donc passé, via le paramètre *adresse*, le URL absolu de la ressource demandée. Pour rendre cet URL absolu, une fonction du module Perl URI::URL a été utilisé. C'est donc en modifiant tous les URL d'un fichier HTML de cette façon qu'on peut garder un



• Figure : flot d'information

utilisateur en mode proxy. La figure précédente résume cette façon de faire.

Définition des paramètres

En plus de l'adresse de la ressource originale, proxy.pl accepte plusieurs autres paramètres. Par exemple, le code zébré de l'utilisateur sera conservé et repassé à proxy à chaque requête. Voici donc la liste de tous les paramètres que proxy accepte :

Paramètre	Définition
adresse	L'URL d'une ressource.
codebarre	Le numéro de dossier (code zébré) de l'utilisateur qui fait la requête.
parse	Opérateur booléen. Donner la valeur 0 à parse demande à proxy de renvoyer le fichier HTML sans modifier les liens. Par défaut, parse vaut 1, donc les liens sont modifiés. On verra l'utilité de ce paramètre un peu plus tard.
proxyframes	Opérateur booléen. Pour commander à proxy de construire les frames de base de la navigation, on lui donne la valeur 1. Utile seulement lors de la première requête à proxy. Par défaut, proxyframes vaut 0.
Proxymenu	Opérateur booléen. Si proxymenu vaut 1, proxy va simplement envoyer le bandeau de navigation. Par défaut, proxymenu a une valeur de 0.

• Tableau : liste des paramètres

Sécurité

La sécurité du serveur Mandataire peut être vue en deux volets. Le volet utilisateur et le volet ressources. Pour ce qui est de l'utilisateur, l'enjeu est de savoir si le serveur Mandataire a affaire à un utilisateur qui s'est authentifié auprès de Portail. Du côté des ressources, il faut s'assurer que le serveur Mandataire est utilisé aux fins pour lesquelles on l'a mis en place. Il ne faut pas oublier qu'au départ, le serveur Mandataire va servir à nos membres pour interroger les banques de données de la Bibliothèque à distance.

Les utilisateurs authentifiés

Lorsqu'un utilisateur désire interroger une banque et se trouve en dehors du campus (à la maison, par ligne PPP d'un fournisseur commercial, par exemple), il est amené devant Portail. Portail est un système d'authentification déjà en place à la Bibliothèque qui vérifie dans la base de données institutionnelle la validité du code à barres et du NIP. Quand l'utilisateur s'est identifié auprès de Portail, Portail va porter le code à barre de cet utilisateur dans un fichier d'utilisateurs authentifiés. Ce fichier possède physiquement le chemin suivant : E:\proxy\usagers.txt. Le programme proxy.pl est ensuite appelé pour la première fois en spécifiant l'adresse de la ressource que l'utilisateur a originalement demandée, le numéro de dossier de l'utilisateur et le paramètre proxyframes avec la valeur 1. Prenons comme ressource originale Current Contents et comme numéro de dossier 012345678. Techniquement, Portail effectue une requête HTTP de l'adresse suivante :

```
http://proxy.bibl.ulaval.ca/cgi-
bin/proxy.pl?adresse=http://www.bibl.ulaval.ca/cc&codebarre=0
12345678&proxyframes=1
```

Le serveur Mandataire, lui, une fois appelé, va vérifier dans le fichier usagers.txt afin de savoir si l'utilisateur s'est bel et bien authentifié auprès de Portail. Comme dans notre exemple, l'usager possédant le code à barres 012345678 s'est identifié avec succès, le serveur Mandataire va effectuer la requête auprès du serveur Web de la bibliothèque pour obtenir la page d'accueil de Current Contents, va modifier les liens dans le fichier HTML et va retourner le tout, au navigateur Web de l'utilisateur, formatté avec des cadres puisque le paramètre proxyframes a été passé avec la valeur 1.

Après un délai de 3 heures, un autre programme Perl, menage_usager_proxy.pl, va effacer le numéro de dossier du fichier usagers.txt. Après quoi, l'utilisateur devra retourner s'identifier auprès de Portail, sans quoi, le serveur Mandataire lui refusera la navigation.

Les ressources disponibles par le serveur Mandataire

En plus de vérifier l'identité des utilisateurs, Le serveur Mandataire possède un mécanisme de contrôle des URL demandés. Ces URL sont classés dans trois catégories :

1) Les URL permis

2) Les URL défendus

3) Les URL strictement défendus

À la première catégorie se rattache un fichier texte, comme dans le cas des usagers, E:\proxy\url_proxy.txt. Ce fichier contient simplement l'adresse IP numérique ou alphanumérique des serveurs auxquels le serveur Mandataire peut faire des requêtes. Par exemple, si on désire permettre aux utilisateurs de consulter le site Web de la Bibliothèque en « mode proxy », il suffit d'ajouter les lignes suivantes dans le fichier url_proxy.txt :

```
# Bibliothèque de L'Université Laval
www.bibl.ulaval.ca
```

À noter que les lignes qui débutent par le caractère « # » sont considérées comme contenant des commentaires et ne sont donc pas traitées par le serveur Mandataire.

Il est possible de permettre la navigation à un domaine entier :

```
# Université Laval au complet
ulaval.ca
```

ulaval.ca peut aussi se traduire par 132.203, qui est le domaine IP de l'Université :

```
# Tous les numéros IP de l'Université Laval
132.203
```

Le fichier url_proxy.txt est donc composé des adresses de toutes les pages Web particulières, de tous les serveurs et de tous les domaines qu'on désire permettre aux utilisateurs de visiter en « mode proxy ».

La seconde catégorie est dépendante de la première. Les adresses qui sont défendues sont simplement toutes les adresses qui ne sont pas dans le fichier url_proxy.txt. Il est important de noter que lorsqu'on appelle le serveur Mandataire avec une adresse défendue, il n'affichera pas un message d'erreur, il ira chercher le fichier HTML mais ne modifiera pas les liens. Il se comportera donc comme si on l'avait appelé avec le paramètre parse à 0. Cela implique que la poursuite de la navigation ne se fera plus par l'intermédiaire du serveur Mandataire, et c'est tant mieux, parce qu'il ne faudrait pas que le serveur Mandataire devienne un serveur de navigation Web anonyme.

Il faut aussi savoir que cette manière de fonctionner n'est pas totalement sécuritaire et qu'elle permet tout de même à un utilisateur futé de naviguer de manière anonyme. Comme on le sait, on peut appeler le serveur Mandataire en lui spécifiant une adresse et un numéro de dossier en paramètre. Un usager patient, mais qui désire garder l'anonymat sur un site en particulier, qui ne fait pas partie du fichier des adresses permises, peut simplement appeler le serveur Mandataire avec les URL originaux au lieu de cliquer sur les liens dans son navigateur Web. À chaque fois il obtiendra la ressource non modifiée, mais il lui suffira de répéter la procédure pour naviguer en « mode proxy » n'importe où. Il s'agit là du principal inconvénient dans le fait de ne pas afficher un message d'erreur quand une ressource défendue est demandée, mais c'est aussi un compromis qu'il faut faire pour ne pas trop ennuyer les utilisateurs qui se servent du serveur Mandataire avec des buts plus légitimes.

La troisième catégorie va permettre de corriger un peu la faille de sécurité que la seconde crée. Les adresses strictement défendues se retrouvent dans le fichier E:\proxy\url_noproxy.txt. Si le serveur Mandataire rencontre un URL qui contient l'adresse d'une ressource strictement défendue, il affichera un message d'erreur et n'effectuera pas la requête. Il peut être très pratique d'intégrer à ce fichier les adresses des sites ou des pages Web particulières dont on ne doit absolument pas donner accès, même si on ne modifie pas les liens. Pensons à Chemical Abstracts, banque pour laquelle la Bibliothèque possède une licence qui ne lui permet pas de diffuser en dehors du campus. Comme le lien vers Chemical Abstracts appelle directement le plugin Metaframe, il ne faut pas du tout faire la requête car dans ce cas, ce n'est pas une page HTML qui est appelée mais bien une application qui s'exécute, il faut donc bloquer l'accès directement.

On ajoute une ligne dans url_noproxy.txt tout comme dans url_proxy.txt :

```
# Chemical Abstracts, accès interdit pas proxy
www2.bibl.ulaval.ca/bd/chemabs/
```

C'est donc grâce à ces deux dispositifs de sécurité qu'il est possible de contrôler les accès au serveur Mandataire. Évidemment, comme les besoins évoluent, il sera peut-être utile à l'avenir de renforcer ces dispositifs.

Le fichier LOG

Le fichier LOG est un moyen de vérifier qui a utilisé le serveur Mandataire, quand et pour accéder à quelle ressource. Les informations relatives à un accès se retrouvent toutes sur la même ligne, présentée ainsi :

```
JJJ_MMM_DD_HH:MM:SS_<Navigateur>_<Adresse IP du client>_<URL
demandé>
```

Le caractère souligné représente ici un espace. JJJ est l'abréviation du jour de la semaine en anglais sur 3 caractères, MMM est l'abréviation du nom du mois en anglais sur 3 caractères et DD représente la date actuelle, sur 2 chiffres. HH:MM:SS représente l'heure en heures, en minutes et en secondes.

Le fichier LOG pourra être très utile pour retracer des utilisateurs un peu trop futés ou plus prosaïquement pour créer des statistiques d'utilisation.

Exception

Afin de faciliter les tests et de donner une porte d'entrée facile au programmeur, le code à barre 111111111 peut-être utilisé pour naviguer en « mode proxy ». En effet, le serveur Mandataire va permettre de naviguer avec ce code si l'utilisateur se trouve dans le domaine 132.203. Il est donc nécessaire de se trouver sur le campus pour accéder à au serveur Mandataire de cette manière. Il est aussi recommandé de changer souvent ce code à barre de tests directement dans le script proxy.pl pour qu'il ne tombe pas entre les mains de n'importe qui.

L'interface utilisateur

L'interface utilisateur est relativement simple. À la base, il s'agit de la même interface que l'utilisateur a l'habitude de rencontrer quand il naviguc sur le Web, soit l'interface offerte par son navigateur Web. À cela, on a ajouté une sorte de bandeau, qui est en fait un cadre créé lors du premier accès au serveur Mandataire, après authentification auprès de Portail. Dans le second cadre, c'est-à-dire sous le bandeau, se fera la navigation Web en « mode proxy ». À chaque fois que l'utilisateur clic sur un lien, c'est dans ce cadre que la ressource lui sera présentée.

Le bandeau contient de l'information et des icônes. Pour que l'utilisateur sache qu'il est bien en train d'accéder à des ressources via notre serveur Mandataire, nous l'en informons. Dans le bandeau, on a inscrit : « NAVIGATION EN MODE PROXY » à gauche.

Dans l'extrémité droite du bandeau, on a inséré trois icônes. Le premier représente une petite maison. Un clic sur cet icône chargera la page d'accueil de la Bibliothèque dans le cadre de navigation principal. Le second icône est un point d'interrogation. Un clic sur cet icône chargera une page d'aide dans le cadre de navigation principal. Le troisième icône représente un panneau de signalisation arrêt. Un clic sur cet icône provoquera la fin de la session de travail et le serveur Mandataire signalera à l'utilisateur que la navigation en « mode proxy » est terminée. Le serveur Mandataire enlèvera le code à barre de l'utilisateur du fichier usagers.txt et l'utilisateur devra donc retourner devant Portail s'il désire recommencer à naviguer en « mode proxy ». Évidemment, il n'est pas nécessaire de se débrancher du serveur Mandataire de cette manière puisque la session sera automatiquement terminée après trois heures, mais il est néanmoins recommandé de le faire.

Le code source du script proxy.pl, lignes à lignes

Afin de rendre facile l'ajout ou la modification de code dans le script proxy.pl, voici une description du programme lignes par lignes.

21 à 23 : Message d'erreur standard qui sera utilisé à toutes les sauces dans le programme.

25 à 29 : Déclaration des modules à utiliser dans le programme

31 à 39 : Déclaration de plusieurs variables qui seront utiles pendant l'exécution.

41 : Création d'un objet CGI. Cet objet va contenir, entre autre, les paramètres passés à proxy.pl.

42 : Récupération des noms des paramètres dans le tableau @in.

43 à 48 : Sauvegarde des paramètres dans deux variables spéciales pour utilisation ultérieure pendant l'exécution. Le tableau référentiel %in (en anglais, Hash Table) contiendra les paramètres sous la forme de paires clé-valeur. Pour obtenir la valeur du paramètre adresse , par exemple, il s'agira de le référencer de cette manière : $in{'adresse'}. La deuxième manière de sauvegarder les paramètres est de créer un tableau de références plat. En fait, il ne s'agit que de modifier chacune des entrées de

@in en lui concaténant le symbole « = » et la valeur du paramètre. En anglais, on peut appeler cette construction un Flat Hash. L'entrée correspondant au paramètre adresse, par exemple, va ressembler à ceci : adresse=http://www.bibl.ulaval.ca/. Cette manière de sauvegarder les paramètres va être utile quand on voudra reconstruire les paramètres de la requête originale dans une nouvelle requête GET.

50 à 59 : Ce bout de code vérifie que la requête provient de Portail. Dans ce cas, proxy ajoute le code à barre dans le fichier usagers.txt. Une ligne est aussi ajoutée dans le fichier LOG. Cette procédure est une faille dans la sécurité de proxy, mais aussitôt que possible, elle sera transférée dans le programme portail pour éliminer la faille.

62 et 63 : On conserve dans des variables l'adresse IP du client et le type de navigateur du client.

65 et 66 : Récupération dans deux tableaux de la liste des URL permis et des URL strictement défendus. Ils seront utiles plus tard quand on voudra comparer avec l'URL demandé.

56 à 64 : Lecture du paramètre adresse. S'il n'y a pas d'adresse de définie dans les paramètres, la navigation proxy débute sur le site Web de la Bibliothèque http://www.bibl.ulaval.ca/. On élimine adresse des paramètres car lors de la reconstruction de la requête originale, on veut envoyer au serveur seulement les paramètres originaux de la requête. La fonction delete, qui sert à enlever un élément d'un tableau référentiel, est utilisée pour ce faire. À noter que s'il y a des espaces dans l'adresse, ils sont remplacés par le symbole « + ».

66 à 69 : Écriture d'une entrée au fichier LOG. Le fichier LOG est ouvert en mode ajout afin que la nouvelle entrée soit ajoutée à toutes les autres entrées déjà existantes, sur une nouvelle ligne. La fonction &dateetheure va formatter l'heure et la date correctement pour les insérer dans la ligne à écrire. Voir la section 2.3 pour une description détaillée du fichier LOG.

71 à 78 : On vérifie s'il y a un code à barres dans les paramètres. S'il n'y a pas de code à barres, l'accès à Proxy est refusé. Tout comme le paramètre adresse le code à barre est enlevé du tableau référentiel des paramètres avec la fonction delete.

80 à 87 : Vérification du paramètre parse. Pour une description du paramètre parse, voir la section 1.1. Parse est aussi enlevé des paramètres avec la commande delete. Dans le cas où parse ne ferait pas partie des paramètres, on lui donne la valeur 1, afin que la ressource soit modifiée.

89 et 90 : On appelle la fonction &Verif_Usager qui vérifie si le code à barre est bien dans le fichier usagers.txt. S'il ne s'y trouve pas, on bloque l'accès à proxy et on envoie un message d'erreur.

92 à 94 : On vérifie avec la fonction &Verif_URL si l'adresse demandée correspond à une entrée de la liste des adresses strictement défendues. Si c'est le cas, on bloque l'accès et on envoie un message d'erreur.

95 à 101 : S'exécute si la &fonction Verif_URL nous indique que l'adresse ne correspond à aucune entrée du fichier des adresse permises. Dans ce cas, une requête est effectuée, mais aucune modification n'est apportée à la ressource demandée, seul un élément HTML est ajouté, il s'agit de <base>, afin que les images du fichier HTML retourné s'affichent correctement. La commande exit(1) termine ensuite le processus.

103 à 111 : On récupère le paramètre proxyframes. S'il a la valeur 1, on envoie les frames au navigateur client et on termine le processus avec exit(1). À noter que l'attribut src de l'élément représentant le premier cadre (le bandeau) est une référence à proxy.pl avec le paramètre proxymenu à 1. Ainsi, une fois proxy appelé avec ce paramètre, les lignes 113 à 121 afficheront le menu dans ce cadre. L'attribut src du second cadre contient un appel à proxy.pl avec en paramètre l'adresse de la ressource demandée. Le paramètre proxyframes est enlevé avec la fonction delete s'il vaut 0.

113 à 121 : Vérification du paramètre proxymenu. S'il vaut 1, on envoie le menu Proxy au navigateur client et on termine le processus avec exit(1). S'il vaut 0, on enlève proxymenu des paramètres avec la fonction delete.

123 : Après toutes les vérifications précédentes, on peut finalement exécuter la requête pour le client. Les détails de la fonction &Requete sont expliqués de la ligne 168 à 260.

125 à 130 : On détermine le URL de base de la ressource qui a été récupérée par la requête de la ligne 123. Il a fallu inclure un cas spécial: IBM Patent Server. Le serveur envoie un header Location incorrect contenant index.html. Le URL de base ne serait donc pas valide. Il faut corriger cette erreur du site Web de IBM afin que les images s'affichent correctement et que les liens modifiés soient valides. Si jamais l'URL de ce serveur change, il ne faudra pas oublier de changer ce bout de code en même temps.

132 : À partir d'ici commence le traitement principal de la requête effectuée. La ligne 132 vérifie si la ressource est bien un fichier HTML et si le paramètre parse vaut bien 1. L'affirmative nous amène à la ligne 133, dans le cas contraire, nous aboutirons à la ligne 152.

133 à 140 : On vérifie si la récupération du fichier HTML s'est effectuée avec succès, on envoie les headers de la requête au navigateur client et on crée un objet MyFilter qui va effectuer les modifications au contenu du fichier HTML et les envoyer au navigateur client. La ligne 136 indique à Perl qu'il y a du code de défini après le marqueur __END__ de la ligne 410, sans quoi la classe MyFilter ne serait pas prise en compte par l'interpréteur Perl. La ligne 137 crée l'objet MyFilter en lui assignant la valeur des variables $BASE, qui contient l'adresse de base de la requête, $ajout, qui contient l'adresse de proxy et $codebarre. La ligne 138 et 139 activent l'objet MyFilter avec le contenu du fichier temporaire contenant le code HTML de la ressource. Ce fichier est créé par la fonction &Requete.

141 à 150 : On arrive ici si la requête n'a pas été effectuée avec succès. Dans ce cas, il peut se produire deux choses : lignes 142 à 146, le code d'erreur associé à la requête est 302, il s'agit d'une redirection qui n'a pas été traitée. Dans ce cas il faut simplement modifier le header Location pour qu'il pointe vers Proxy, ainsi, le navigateur va récupérer la bonne ressource. Lignes 147 à 149, le programme ne gère pas l'erreur qui s'est produite et envoie simplement un message d'erreur au navigateur client. Aux fins de déboguage, la ligne 148 affiche le code d'erreur et le message d'erreur dans le navigateur.

152 à 154 : On arrive ici dans le cas d'une ressource autre qu'un fichier HTML ou si le paramètre parse a été passé avec la valeur 0. On envoie tout simplement la ressource originale au navigateur client.

156 et 157 : On détruit les fichiers temporaires créés durant le processus.

159 : Le programme se termine avec succès.

168 : Fonction &Requete.

170 : Récupération de la méthode passée en argument.

171 : Création d'un objet UserAgent, qui va effectuer la requête HTTP.

173 : Vérifie si on a affaire à une méthode GET. Dans ce cas, les lignes 174 à 198 sont exécutées, sinon, la ligne 199 vérifie si on a affaire à une méthode POST, si c'est le cas, ce sont les lignes 200 à 222 sont exécutées, sinon, Proxy a été appelé avec une méthode qui n'est pas gérée et on envoie un message d'erreur au navigateur client.

174 à 184 : Reconstruction des paramètres de la requête. Pour ce faire, on utilise le Flat Hash. On débute la chaîne de paramètres $query_string par un « ? », on ajoute ensuite chacun des paramètres différents d'adresse et de codebarre, suivi du caractère « & ». Les lignes 181 à 183 vérifient si la chaîne de paramètres ne contient que le « ? », dans ce cas la chaîne ne contient pas de paramètres, on lui assigne une chaîne vide.

185 à 187 : Vérifie simplement que la chaîne de paramètres ne se termine pas par un « & », dans ce cas, on l'enlève parce que ça signifierait envoyer un paramètre vide avec une valeur vide, ce qui n'est pas souhaitable.

188 : Création d'un nouvel objet Request, qui contiendra toutes les informations au sujet de notre requête. On lui assigne dès le départ l'adresse de la ressource demandée ainsi que la chaîne de paramètres reconstruite aux lignes 174 à 187.

189 : Initialise le header User-Agent de la requête avec le type de navigateur du client.

190 : On informe aussi l'objet UserAgent du type de navigateur client afin que le serveur sache à quel genre de navigateur il a affaire.

191 : Comme il faut conserver les cookies de la requête au cas ou le serveur nous les demanderais, cette ligne crée un objet Cookie qui stockera les biscuits dans le fichier cookies.txt. À remarquer qu'il est important d'assigner la valeur 1 à l'argument ignore_discard pour que tous les cookies soient conservés, même ceux que le serveur ne désire pas que nous conservions. Si on ne le fait pas, les cookies habituellement conservés en mémoire vive par Netscape seront perdus et certaines requêtes seraient alors faites hors contexte, ce qui pourrait avoir des effets bizarres.

192 : On informe l'objet UserAgent qu'il a maintenant une jarre à biscuits à sa disposition.

193 : Et que cette jarre à biscuits se trouve dans le fichier cookies.txt.

194 : À l'objet Request, on greffe les cookies trouvés dans la jarre qui lui sont pertinents.

195 : Et après tous ces préparatifs, on effectue finalement la requête. À noter ici que l'on n'a pas besoin de créer un objet Response. Cet objet est automatiquement crée par le UserAgent et retourné dans la variable $res.

196 et 197 : Les cookies reçus sont extraits et rangés dans la jarre.

199 : Vérifie si on a affaire à une requête POST.

200 : Vérifie si le type d'encodage des paramètres est multipart/form-data. Dans ce cas, exécute les lignes 201 à 205, sinon les lignes 206 à 221.

201 : Requiert les services du module HTTP::Request::Common qui est en mesure de traiter les paramètres multipart.

202 : Cette ligne effectue une opération étrange, elle transforme le tableau de références %in en variable référentielle à un Hash. Cette étape est par contre essentielle parce que c'est sous cette forme que les paramètres seront passés à la requête.

203 et 204 : On effectue la requête sans gérer les cookies. Il serait préférable de le faire, mais comme le problème est assez complexe, il n'a pas encore été résolu. À faire dans un avenir proche. À noter la manière dont on initialise les différents headers de la requête, dont on passe les paramètres et dont on assigne l'adresse de la ressource dans le cas d'un objet HTTP::Request::Common. Tout se fait dans la même instruction.

206 : Le type d'encodage n'est pas multipart, on suppose donc qu'il s'agit de www-form-urlencoded, le type d'encodage par défaut.

207 : Crée l'objet Request et lui assigne l'adresse de la ressource. Les paramètres seront passés ultérieurement.

208 : Initialise le header Content-Type avec le type d'encodage utlisé.

209 : Crée un objet URL de type HTTP.

210 : À cet objet URL, on greffe les paramètres de la requête contenus dans le tableau référentiel %in.

211 : Les paramètres aboutissent finalement dans le contenu de la requête. Pour les passer à l'objet Request, on utilise la méthode equery de l'objet URL qui « escape » les caractère non-ascii et les caractère spéciaux contenus dans les paramètres.

212 à 220 : idem aux lignes 189 à 197.

223 à 225 : On a appelé Proxy avec une méthode non gérée, un message d'erreur est envoyé au navigateur client.

227 à 229 : Sauvegarde les headers de la réponse dans un fichier temporaire.

231 à 237 : Vérifie le type mime de la réponse et la sauvegarde dans une variable. Si les headers de la réponse ne contenaient pas de type mime, on lui donne text/html par défaut. Cette opération est importante puisqu'il faut savoir si on doit modifier le contenu de la ressource.

239 à 243 : On enlève les headers X-Meta et Content-Length des headers qui seront retournés au navigateur. C'est pour éviter justement que le header Content-Length ne contiennent une valeur erronée après modification de la ressource.

245 à 250 : Sauvegarde le contenu de la réponse dans un fichier temporaire qui sera utilisé par la suite. À noter les lignes 247 et 248 qui ajoutent des marqueurs de commentaires quand il y a des scripts dans le fichier HTML.

252 à 260 : Dernière partie de la fonction &Requete qui vérifie s'il y a un header META avec l'instruction REFRESH dans le fichier HTML. Si c'est le cas, la fonction &Requete devient réentrante jusqu'à ce qu'il n'y ai plus de REFRESH à traiter. ATTENTION : cette partie du programme est peut-être dangereuse. Je ne l'ai pas testée en profondeur et il

est possible que le programme entre dans une boucle sans fin si jamais le REFRESH pointe toujours vers le même fichier. C'est à vérifier.

268 à 289 : La fonction &Print_Frames qui génère le fichier HTML des frames de la navigation en mode Proxy.

297 à 321 : La fonction &Print_Menu qui génère le fichier HTML du menu de Proxy.

329 : La fonction &Lire_URL.

330 : Récupère le nom du fichier à lire des arguments.

331 : Tableau temporaire qui va contenir la liste des URL.

332 à 339 : Lecture du fichier et stockage de la liste des URL. On stock chaque URL deux fois : une fois sous sa forme originale et une fois sous sa forme « escape ». Ceci est du au fait que l'objet MyFilter « escape » les URL originaux avant de modifier les liens dans le fichier HTML. Il faut donc pouvoir comparer des pommes avec des pommes et des oranges avec des oranges. À noter la ligne 334 qui élimine les lignes débutant par « # ». Ces lignes ne sont que des commentaires dans le fichier.

341 : On retourne le tableau contenant tous les URL lus.

350 à 360 : Fonction &Verif_URL qui vérifie si l'adresse de la requête correspond à une des entrées du tableau des URL passé en argument. Retourne 1 si c'est positif, 0 dans le cas négatif.

368 : Fonction &Verif_Usager.

369 : Récupère le nom du fichier des usagers et le code à barres à vérifier.

370 : On définit un tableau temporaire et l'opérateur booléen.

371 à 377 : Lecture des codes à barres contenus dans le fichier des usagers authentifiés, stockage dans le tableau temporaire.

378 et 379 : Vérifie si le code à barres 111111111 est utilisé. Dans ce cas, l'usager est valide si l'adresse du client fait partie du domaine 132.203.

380 à 383 : Si on trouve le code à barres dans le fichier des usagers authentifiés, l'usager est valide.

384 : On retourne l'opérateur booléen qui vaut 1 quand l'usager est valide et 0 s'il est invalide.

393 à 408 : La fonction &dateetheure qui imprime simplement la date et l'heure dans le fichier LOG. La ligne 394 initialise la structure localtime avec la date et l'heure présente, les lignes 395 à 401 récupèrent chacun des éléments de la structure dans des variables plus faciles à reconnaître et les lignes 402 à 407 impriment la date formatée comme on le désire. Bogue de l'an 2000, hé oui, on ne peut y échapper : si l'année est < que 2000, il faut ajouter le 19... (sinon la date ne s'afficherait que sur 2 caractères : 99 par exemple).

410 : Marqueur de fin du programme. Dépassé cette ligne, rien n'est interprété si on ne le spécifie pas dans le programme.

419 : Début de la nouvelle classe MyFilter, dérivée de HTML::Filter. Cette nouvelle classe a été modelée à partir d'un programme de Randal L. Schwartz disponible à l'URL : http://www.stonehenge.com/merlyn/WebTechniques/col32.html

420 à 422 : Modules qui contiennent certaines méthodes qui seront utiles.

425 et 426 : Ces lignes étaient là et n'ont pas été modifiées.

427 et 429 : 4 variables globales à l'objet et qui seront utiles.

431 à 438 : Hash des éléments qui contiennent des URL qui devront être modifiés pour pointer vers Proxy.

440 à 447 : Hash des éléments qui contiennent des URL qui devront simplement devenir absolus.

449 à 463 : Ce bout de code transforme chacun des Hash en Flat Hash. C'est un tour de passe-passe assez complexe qu'il n'est pas nécessaire d'expliquer.

465 à 472 : à la création de l'objet, on définit trois choses : $self->{Url} qui est en fait l'adresse de base de la ressource, $self->{ScriptName} qui contient la valeur de la variable $ajout définie au tout début du programme et $self->{CodeBarre} qui est le code à barres de l'utilisateur authentifié.

475 à 478 : Ces quelques lignes n'ont pas été modifiées du programme original et ne devraient pas avoir besoin de l'être parce qu'on ne désire pas modifier les déclarations, les commentaires et les zones de texte dans le fichier HTML.

480 à 493: La méthode end qui est appelée quand l'objet MyFilter rencontre un élément de fermeture HTML. Si l'élément </FORM> est rencontré, il faut ajouter deux champs <HIDDEN> au formulaire. Ces champs contiennent l'adresse originale de l'attribut action du formulaire qui a été remplacé par l'adresse de Proxy et le code à barres de l'utilisateur authentifié. Il est extrêmement important d'ajouter ces deux champs parce que lorsque le formulaire sera envoyé, Proxy va le recevoir et doit connaître l'URL original ainsi que le code à barres de l'utilisateur afin de pouvoir effectuer la requête correctement. Si jamais le fichier HTML contient un élément de départ <FORM> mais pas d'élément de fermeture </FORM> (et ça peut arriver, mauvais codage HTML par l'auteur!!!), il faut quand même insérer les 2 champs <HIDDEN>. Les lignes 286 à 491 voient dans ce cas à les insérer et corrigent même le code HTML en lui ajoutant l'élément de fermeture </FORM>.

495 : La méthode start. C'est le cœur de l'objet MyFilter. C'est ici que la modification des URL se fait dans les éléments HTML de départ. À chaque fois qu'un élément de départ est rencontré dans le fichier HTML cette méthode est appelée. Nous n'allons traiter que les éléments stockés dans les Flat Hash construits à la ligne 449.

496 : Le premier argument envoyé à une méthode d'un objet est en général le pointeur à cet objet. On le récupère avec la fonction shift, qui sans argument va s'appliquer à la variable @_, tableau qui contient tous les arguments passés. Shift ramasse l'argument et l'enlève du tableau, comme si on faisait un pop sur une pile.

497 Récupère les 4 prochains arguments dans 4 variables.

498 Définition de deux variables qui seront utiles.

499 à 501 : Construction d'une table de caractère d'échappement qui va permettre d' « escaper » l'adresse de la ressource qu'on va placer en paramètre de proxy.pl dans les URL modifiés. D'habitude on se sert de la méthode uri_escape du module URI::URL pour ce faire, mais étrangement, ça entre en conflit avec notre nouvelle classe dans ce cas-ci.

502 : On commence à réécrire l'élément HTML en imprimant < et le nom de l'élément contenu dans $tag.

503 : Pour chacun des attributs de l'élément, on exécute les lignes 504 à 541.

504 : On imprime le nom de l'attribut et le symbole « = » et un guillemet.

505 : On se définit une variable temporaire $val qui correspond à une chaîne vide.

506 à 508 : Si la valeur de l'attribut est différente de la chaîne « value », on copie cette valeur dans $val. Cette opération est nécessaire parce que dans le code html de certains sites, aux attributs value de certains champs de saisie est associé une valeur « value » sans guillemet qui est interprétée correctement par Netscape, mais notre méthode start corrige le HTML et ajoute des guillemets pour chacun des attributs, après quoi, la valeur « value » entre guillemet est interprétée par Netscape littéralement et le formulaire devient alors incorrect. Ça peut sembler compliqué, mais si on enlève ce bout de code préventif, on comprend vite pourquoi il a été ajouté.

509 à 511 : Ici on vérifie si l'élément et l'attribut font partie de la liste des éléments dont l'URL doit être rendu absolu. Si c'est le cas, la ligne 510 se charge du travail.

512 : Vérification e l'élément et de l'attribut une seconde fois. S'ils font partie de la liste des éléments dont l'URL doit être entièrement réécrit, alors on va exécuter les lignes 513 à 537.

513 : Si l'URL est un point d'ancrage (« anchor » en anglais) on ne lui touche pas.

514 à 519 : Si c'est un appel à la fonction javascript MkUniq des pages HTML de Proquest Direct, on va opérer certaines modifications à l'URL passé en argument à cette fonction. Cette opération très délicate est nécessaire afin que le code javascript de Proquest demeure opérationnel.

520 à 522 : Si l'URL est une référence à un fichier de définition d'une image map, on le rend simplement absolu.

523 à 527 : Si on a affaire à un élément <FORM> on change l'URL d'action pour l'URL de proxy. On assigne l'URL original du formulaire à la variable $adresse, qui sera utilisée ultérieurement pour construire un champ <HIDDEN>.

528 à 536 : Il faut reconstruire totalement l'URL. Dans l'ordre, les morceaux du nouvel URL sont : L'adresse de Proxy, le paramètre adresse avec l'adresse originale de la ressource rendu absolu et sous forme de chaîne « escapée » et le paramètre codebarre avec le code à barres de l'utilisateur authentifié.

539 et 540 impriment finalement l'URL modifié, en encodant les caractère >< et & qu'il peut contenir.

542 : Termine d'imprimer l'élément avec la caractère >.

543 à 546 : Si on a rencontré l'élément formulaire, il faut construire les deux champs <HIDDEN> qui sont imprimés à la ligne 480.

547 à 549 : Dans le cas de Proquest Direct seulement, on ajoute un élément <BASE> dans le header du fichier HTML avec le URL de base de Proquest. Ceci encore dans le but de permettre au javascript des pages de Proquest de fonctionner correctement.

Statistiques

Dans la section sur la sécurité, il a été vu que le serveur Mandataire créait un fichier LOG de toutes les requêtes effectuées. C'est à partir de ce fichier que les statistiques sont compilées par un script Perl appelé compile.pl. Ce programme compile les données relatives au navigateur utilisé par rapport au nombre de requêtes effectuées, au numéro IP du client par rapport au nombre de requêtes effectuées, au numéro de dossier du client par rapport au nombre d'authentifications faites auprès du service Portail et à la ressource utilisée par le client à savoir s'il s'agit d'un serveur interne à la bibliothèque ou d'un serveur externe. Le fichier des statistiques compilées (statistiques.txt) ressemble à ceci :

```
# Navigateurs
Mozilla/4.0=256
# Numéros IP
123.123.123.123=23
# Login usagers
012345678=1
# Ressource consultée
externe=5555
interne=5555
```

Évidemment, le fichier réel contient beaucoup plus de types de navigateurs, de numéros IP et de numéros de dossiers différents.

Un autre script Perl (stats_proxy.pl) permet de visionner les statistiques compilées dans un navigateur Web comme Netscape. Les données sont alors présentées sous forme de tableau pour en faciliter la lecture. On peut les consulter à l'adresse : http://proxy.bibl.ulaval.ca/cgi-bin/stats_proxy.pl

Project Plans

University of Connecticut

University ITS

Authentication Project -

Index

University ITS

UConnWeb

Welcome to University Information Technology Services.

In addition to many other services, University ITS is developing a campus-wide authentication system that will allow a single username and password to be used on most University services.

Authentication Project Profile
The Project Profile defines the scope, phases and resource requirements of the Authentication project. It is a good starting point to understand how UConn's project is defined and how it relates to Single-Sign-On, Portals, email, groupware and other current issues.

Policy Issues & Frequently Asked Questions
Part of bringing together many different information technology systems under a common username and password umbrella is developing policies that address security, privacy, management and technology issues for the many users. This addresses policy and provides an opportunity to comment on the UConn initiative.

Project Timeline and Task Assignments
The timeline is a working document that defines critical project milestones for the project. This page also shows which group is responsible for each project associated task.

Research, Development, Prototyping
As the team evaluates solutions and their integration with existing technologies at the University, updates are added here to document the research.

To access your Lotus account on the web, click here.
To access your Login to Exchange, click here.

Last updated 9/3/01
Mail comments to: *Rob.Vietzke@uconn.edu*

UConnWe

University of Connecticut

University ITS

Authentication Project

Index

University ITS

UConnWeb

Authentication Project Profile

Project Profile

Project Title: Authentication, Authorization and Security Project

Project ID#: None

Budget Period: FY2001-FY2004

Project Profile Date: June 1, 2001

Project Description: The Authentication and Authorization project is a strategic initiative of the Information Technology Steering Council and UITS. It is intended to reduce the number of username and password instances a user at the University must manage and to begin to create a central repository that identifies all users of IT services within the University community. To date, most ID management systems have been functionally related (IE: "Mainframe ID", "Student ID", "Staff ID", "Voicemail PIN", "PPP ID", "WebCT ID", "Exchange ID", "Novell ID", etc.) As the Authentication project evolves, all of these usernames and password instances will be consolidated under a single, and more secure, central database.

The usefulness and acceptability of the system will be in part based on its pervasiveness within the community. This means that any individual who can reasonably claim association with any IT related system at the University will need to be offered an identifier on the system. The implications are that a comprehensive review of the policies that regulate creation, management and use of all University identifiers will be critical to the project's long-term success and sustainability.

Through the ITSC, it has been determined that this will be a multi-year phased effort that ***will initially focus on broad student services including email, library access, file storage, WebCT and calendaring*** .

After the initial project infrastructure is in place, mechanisms to enable distributed authorization off of the central authentication system must be enabled for web based and possibly even legacy based applications at the departmental level.

This project will involve a number of business practice changes throughout ITS and the University to be successful. ***By example, the format of the Universal ID (CMS ID) will likely need to be changed for all faculty and staff. Also, many of the methods through which accounts are added and deleted to various systems will***

need to be refined to allow the separation of username/password authentication management from role and authorization functions.

Program Manager:	Rob Vietzke, Chief System Architect, UITS
Telephone:	(860) 486-3962
E-mail:	Rob.Vietzke@uconn.edu
Fax:	(860) 486-8425

Project Management: Rob Vietzke serves as the overall project manager, currently working approximately 40% on this project and drawing on staff resources that have been requested from other areas of UITS. This profile and previous project outlines ***request four dedicated UITS staff members*** , which is the consensus of project need among both internal and external groups that have reviewed this project profile. Once these resources are in place, one of the dedicated staff members will be asked to assume the role of day to day team leader. This individual will also be responsible for documenting project status on a weekly basis.

The project will be ***divided into three phases, in each phase, prototyping, system development and rollout will occur*** . During the latter portion of one phase, a second phase may startup and run concurrently.

There are three activities related to the Authentication project within UITS. Responsibilities included in this are:

- Core Technical Team – Evaluate technologies and integration issues, prototype solutions, recommend implementation approaches. This team currently includes 3 members of the server support team, allocated on a time/availability basis up to 20%, a University Library IT staff person at 20% and a Law Library staff person at 20%. (Additional staff to grow the project resources to 4 FTE have been requested as part of this and prior project plans.)

- Matt Smith of the server support group is currently responsible for investigating, documenting and recommending a relationship between Windows NT, Windows 2000, Active Directory, and Exchange for use in the LDAP environment.

- Bruce Roy is responsible for installing the C/A LDAP product on top of ACF2 as a possible production LDAP environment for one instance of the authentication mechanism. Bruce is tasked with installing the product in the S/390 environment and then working with Matt and Mitch to test the LDAP schema functionality.

- Mitch Saba is responsible for establishing a working test of the WebCT environment on Solaris against an external LDAP authentication mechanism. Upon successful proof of concept for WebCT, Mitch will be working to establish a conversion plan for the existing WebCT environment.

⊙ Peter Murray is contributing Linux and authentication support to the team on behalf of the Law School. He is primarily working with AIX and LINUX hosts in testing both LDAP clients and server models. Peter will be responsible for testing replication between different LDAP servers once they are in place.

⊙ Steve Weida is responsible for assuring that the prototype environment in UITS would meet the needs of the University Libraries with regards to authenticated resources they may provide. Steve is also investigating the conversion of the electronic course reserves (ECR) onto WebCT after the successful conversion of WebCT authentication.

⊙ Policy Steering Committee – Include a broad cross-section of the University to determine implications and approaches to business-practice related policy issues. Focus is on information dissemintaiton, awareness, and local activities required to implement central policies. This group is chaired by Rob Vietzke, with Elaine David contributing major portions of the policy framework.

Elaine David has been assigned to research, document and coordinate major policy issues related to IT and specifically this project. In her role as policy coordinator, she is looking for best practices related to Authentication at other institutions, adapting them to UConn circumstances, and presenting them to the technical and policy working groups for discussion. Upon vetting in these groups, she will be working to bring these issues to the ITSC for approval.

⊙ ***University ITS Leadership- Manage and coordinate work in functional areas to effect both core system architecture/operation and business practices to effect the new single username/password approach for the systems identified. Specifically, the leadership team will be responsible for coordinating efforts and investing staff resources to accomplish tasks throughout the project. The cross area work will need to be syncronized to assure timely outcomes.***

For this project to be successful, the UITS leadership will needs to examine and determine strategies to increase the 24 availability of the system and services that will serve the Authentication system. Examples of areas for review may include continued automation of account maintenance functions, network availability, server availability, network/server security and weekend support.

The UITS leadership must also coordiante this project with several other projects that will rely on this system for their username/password information. Similarly, this project will depend on several other intitiatives to deliver the initial services requested by the ITSC. By example, Peoplesoft, Email, Groupware, File Storage/Server Consolidation, WebCT, Listserves, Network, and portal initiatives are all heavily intertwined with Authentication and must be managed together for overall cohesion and interoperability.

⊙ *University ITS Functional Areas – Throughout the process, resources in Network, Server, Applications, Database Administration, Help Desk, Operations and Device support will be required to make large contributions to specific portions of the project. The manager's of these areas will be expected to lead the implementation and coordination of efforts within their areas under the general project leadership.*

Initial examples of work that fucntional areas in UITS may need to contribute to this project include:

⊙ *Applications: Creation and support of interfaces from/to existing HR and Student Systems to facilitiate automatic creation of username/password pairs, syncronization of the ID database with the LDAP server, PIN and ID system syncronization, privacy policy application, and interfaces to personal name and list-serve systems.*

⊙ *Help Desk/Accounts: Definition and refinement of policies related to creating and managing authorization to central services,*

⊙ *Network: Creation of a highly-secure "server zone" within the network architecture that can safely allow LDAP server replication and maintenance within the "zone" while also allowing limited user-side access to LDAP lookups and other database queries.*

⊙ *Network: Establishment of service level expectations and definition of redundancies that can be expected for the directory server segments of the network*

⊙ *Server Support: Identification of a preferred platform within the UNIX domain on which the authentication services will run and be most fully supported for a production environment.*

Project Need:

The University currently has dozens of individual username/password and authentication systems spread across departments, divisions and individuals. Many individuals manage five or more usernames/passwords to access the resources they use on a daily basis. The user angst associated with multiple identities also requires multiple administration functions and decreases security by removing any single point of management or policy base for deactivating privileges.

The ITSC has identified this project as a critical strategic need for the University's IT infrastructure to move forward.

Project Benefit:

This project will enable students, administrators, and teachers to work more productively across many systems at the University, without requiring individuals to maintain separate identities within the Community. By simplifying the number of identities maintained within the community, user should be able to remember a more robust set of username and password schemes for their single account, thus increasing security.

As a core component of future services, the authentication system will also enhance the University's ability to rapidly deploy customized services based on individuals.

Project Impact:

- Student, Faculty and Staff users will have a defined, irrevocable identity within the University Community which will allow distributed authorization to many separate IT systems.

- The University will be able to participate in national middleware initiatives, allowing new collaborations of researchers and students across institutions.

Information Tech. Architecture:

Component One : Identity Management and Authentication

The project will be based on one or more open LDAP servers, which will hold basic user information like an individual's Common Name, Preferred Name, Email Address, Street Address, Telephone Number, Fax Number, and Organizational Title, etc. In addition, the LDAP directory will hold a password and some additional authorization attribute fields for a limited number of core University services. The LDAP structure will be based on the standard InetPerson and EduPerson object classes, perhaps with a UconnPerson attribute set added as well.

To address a need to integrate with ACF-2 on the S/390 systems, licensing costs associated with retired identifiers, as well as allow for FERPA related student privacy issues, it is likely that a meta directory will be required with several primary information services feeding it. The metadirectory may be the publicly "exposed" server that offers services like departmental server authorization and web-based directories, whereas the directory servers below the metadirectory may carry more comprehensive base data.

Upon initial deployment, at least one LDAP server will need to receive and resolve feeds from the ID System (HR and Student Systems) as well as patron feeds from the University libraries and potentially other sources. (The Policy working group is actively working to define and refine these requirements.)

The LDAP directory will become a central depository for the identification of users throughout the University. Best practice at other Universities implies that as the LDAP infrastructure is stabilized, the UITS may choose to use the LDAP database to feed the legacy systems, as opposed to the other way around. In this instance, the LDAP database becomes the single central repository of ID information for all University community members.

It is likely that subsequent phases of the project will add tributary servers for additional specialized authorization attributes. It is also likely that some custom programming will be created to integrate services like Microsoft's active directory with the open LDAP server.

Component Two: Authorization and Services

As the directory is developed, key technologies are also being developed to synchronize the LDAP based directory into system tools that can be used for authorizing individuals into particular services. First, links from LDAP into operating system level user-management systems for Windows, Novell, S/390 (ACF2), and Unix/Linux are being researched. Second, web-development tools to allow LDAP resources to be integrated into custom applications will also be researched.

By addressing the integration of the directory into operating-system level user management systems, most of the applications that ride on top of contemporary operating systems will be able to take advantage of the underlying user management systems in the operating systems. In the instance of S/390, an attempt to link LDAP to ACF2 may allow applications level security to be applied to the LDAP based username/password pair.

The prototype should prove that an operating system based integration with the LDAP system should also create a framework for robust web-development using SSL and certificate systems.

Project Schedule: 1/2001 through 6/2003

Phase 1 – Spring 2001 – Summer 2001

Prototyping of WebCT, Email, Calendaring and File Storage for students

Longer term project scope refinement

Identification and draft recommendations of critical university wide policies

Budget and resource allocation to address project needs

Phase 2 – Fall 2001 – Spring 2002

Creation (Replication/Conversion) of Universal ID for all Faculty and Staff

Begin Implementation of student file storage, Web CT, Email & Calendaring

Prototyping of integration of Authentication services with web services

Prototyping of distributed server integration options for NT, 2000, Novell

Phase 3 – Summer 2002 – Fall 2002

"Cutover" of Student accounts to Authentication system for core services **

(** pending budget and staff allocation, could be later.)

"Cutover" of Faculty / Staff accounts to Authentication for core services **

(** pending budget and staff allocation, could be later.)

Availability of Authentication services for centrally based web services

Begin Implementation of distributed server support infrastructure

Project Objectives, Scope and Approach:

The goal is to create a single repository of identities for members of the University community. From the single repository, central services may be both authenticated and authorized. The repository will also enable distributed systems to Authenticate, while allowing local control of authorization on distributed systems throughout the University.

Implementation will require consolidation and conversion of existing disparate username/password systems throughout the institution, starting with identification and adoption of a single User ID standard. As the project expands, any user affiliated with the University who needs access to University IT resources will have to be added to the Authentication ID database.

Project Deliverables:

Based on allocation of budget for this project as defined below and the Email and File Storage initiatives separately under consideration, we expect to meet the following deliverables:

Prototype of WebCT, Email, Calendaring, File Storage Sept 15, 2001

Commur on to University Re: Universal ID Creation Sept 15, 2001

Working en onment for student services ** Dec 1, 2001

(** Pending Budget and staff allocation)

Prototype of web development environment March 1, 2002

Prototype of Novell, NT, 2000 environment May 1, 2002

Working environment for web development July 1, 2002

Working environment for Novell, NT, 2000 integration Sept 15, 2002

Organization:

The University Information Technology Services will take the lead role in coordinating this project. Individual departments who wish to become involved in the project will need to also contribute both technical and functional support to the project as services in their areas are considered for migration into the solution.

As user access to information becomes increasingly reliant on this system, the support of traditional UITS "Accounts Desk" functions into off-shift hours will become increasingly important.

Costs and Funding:

Including FTE Staff allocation, this project will cost $880K, $850K, and $400K for its three-year implementation cycle. For ongoing maintenance, FTE, licensing and other support costs are expected to be approximately $208K per year.

Project Issues:

The largest issues are institutional and organizational support to move this project forward in a timely fashion. This project's success depends on staff allocation, financial allocation and a broad UITS and University-wide cultural commitment to migrate current business practices to work cooperatively around a common identity management system. Significant communication by the UITS and IS senior leadership to continue to encourage faculty, staff and students to adopt the new system will be essential.

The UITS leadership will need to identify the staff and funding resources to begin the significant work described herein immediately in order for the timelines to be met. This project profile will need to be updated regularly to reflect a slower implementation timeline if additional resources are not allocated immediately.

Risk Management:

Network and server design to provide redundancy and security of the system databases will be essential. UITS will need to consider the development of a fire walled "secure" domain in which to house the Directory servers and key tributaries. The availability and reliability of the network itself to provide authentication services will also be critical. If the service is to be broadly adopted by users who currently maintain their own identification and authorization schemes, it is essential that the system is trusted to be secure and is nearly always available. The network and server support teams will need to become actively engaged in this process to assure adequate availability and security.

User expectations already exceed available resources and as such, expectation management will be critical, particularly if limited resources continue to be allocated.

Simultaneous progress and regular communication on the Student Email, Central File Storage and Network Upgrades will also be essential for this project to make its timelines and deadlines.

University of Connecticut ITS

PROJECT COST SUMMARY

agency name: University of Connecticut ITS

project name: Authentication Project

Cost category	Costs FY 2002	Costs FY 2003	Costs FY 2004	Estimated Annual On-going Support Costs
Personnel	4 FTE @ $60,000 plus benefits $300,000	4 FTE @ $60,000 plus benefits $300,000	4 FTE @ $60,000 plus benefits $300,000	2 FTE @ $60,000 plus benefits $150,000
Consultant Services	40,000	40,000	40,000	
Maintenance		25,000	50,000	50,000
Training	10,000	10,000	5,000	5,000
Other Expenses	5,000	5,000	2,500	2,500
IT Equipment Purchase *(including Telecom)*	400,000	400,000	$	$
TOTALS	**$755,000**	**$780,000**	**$397,500**	**$207,500**
Indicate all funding sources	General Fund Federal Fund Capital Other	General Fund Federal Fund Capital Other	General Fund Federal Fu 1 Capital Other	General Fund Federal Fund Capital Other
Estimated Cost Savings	$	$	$	$

BEST COPY AVAILABLE

http://www.ist.uwaterloo.ca/sy/projects/idauth/

Identification, Authentication, and Electronic Commerce

2000-08-07

1997 ID-AUTH Working Group

objective, members, background, etc

1998 ID-AUTH-ECOMM Project

- Purpose and organization
- Objectives
- Stakeholders and scope
- Plans and progress
- 1998-07 RFI: Integration of Identification/Authentication Services on Unix and Microsoft Platforms
- Proposal for Identification/Authentication prototype ... summary, detail
- Project meetings
- 2000-06 final report

Maintained by Roger Watt, IST

92

FINAL REPORT for the ID-AUTH-ECOMM Prototype University of Waterloo

Preface

This document is a final report on the implementation of a Prototype for the Identification, Authentication and E-Commerce Project. A prototype ID-AUTH system has been implemented that replaces the original UWdir Institutional Directory, augments that with an authentication service for the campus at large and provides self service access to UWdir data. The prototype was put into limited production in mid November of 1999 well in advance of the year 2000 changeover (but well behind the original schedule). The old directory service is no more.

The intent here is to fulfill the obligations undertaken in the Post Prototype Commitments -- an evaluation of the goals given in the Objectives of the project, an implementation review to address several questions and finally some recommendations on how we ought to proceed.

It is ***emphatically not our intention*** to terminate our work with UWdir and the continued evolution of the Institutional Directory. Instead we're stopping our current work (briefly) at a natural milestone to examine what we've done (in case there are things we want to do differently -- and there are) and think a little about where we are going (with the release of Windows 2000 there are directions we need to consider).

Accepted: by UCIST 23-June-2000.

FINAL REPORT for the ID-AUTH-ECOMM Prototype University of Waterloo

Introduction

The Objectives for this project (from the 1998 Proposal) were:

> The **ID-AUTH Prototype** is a demonstration project with modest goals -- to *improve* existing processes and services (especially around HR/SIS and UWdir), to *demonstrate* that a central ID-AUTH service is possible and will work (if only for a limited set of applications), to *learn* some things while "getting our feet wet" and finally, to *make recommendations* about how (or if) we ought to proceed. Our plans are to do all of that while incurring minimal risk and minimal financial commitments.
>
> The objective of this prototype is to *prove* that Polaris II can use the ID-AUTH service established -- there is no commitment to deliver this ID-AUTH service to the entire Polaris community by January 1999. The prototype is an opportunity for Polaris II testing (in particular load stressing, scaling tests, etc.) so that a migration can be safely *planned* .
>
> It most definitely is *not* our objective to implement the perfect solution that solves everyone's needs -- that we believe is very difficult, very expensive and likely impossible.

The Prototype has improved the processes around UWdir and especially it's relationship to Human Resources and Registrar's data. The implementation is far simpler than the previous version, data arrives in a more timely fashion, data has been extended to include information required to distinguish users (birth date and gender) and to include information that helps in managing student accounts (we now have data for students on COOP work terms, we have registration status to identify students who have withdrawn). Self service access for users lets them manage data without our intervention (their web page and email address). Self service access for authorized system managers lets them implement users without waiting for data from HR or other sources. Self service access lets these managers create generic listings for Departments and other role based contacts.

The Prototype demonstrates that a central service that identifies users (with an assigned UWuserid) and authenticates them (with traditional password credentials implemented by an NT4 Domain) certainly is possible and will work to integrate several services -- traditional Windows login (and file mounts), controlled access to Web services (eg. UWdir itself and other services like the new Request Tracker within IST) and PAM aware applications (like login, IMAP and POP mail, etc.) on Solaris. Projects like the Electronic Voting and the Network Authentication Project build on the authentication service we have established.

The *"Lessons Learned"* and *"Recommendations"* are covered in separate sections of this report.

Our relationship with Waterloo Polaris is not so clear. Very early in the implementation Polaris developers found a Radius solution that integrated the Watstar servers with their

Unix authentication servers. They've come to rely on Pluggable Authentication Module (PAM) services on Solaris systems (using Radius) similar to our use of PAM on Solaris to authenticate against the NT4 Domain using Server Message Block (SMB) Protocols. While it's clear that the ID-AUTH prototype could have provided the Radius service that Polaris relies on (there are lots of Radius implementations on NT) we certainly could not have provided it when they needed it -- our prototype was delivered a year late (sic!). In any case, now that the prototype is in limited production, it's clear that Windows 2000 sets a direction where we acknowledge that there's no need for Radius stress tests (or the soon to be obsolete NT4 Domain) -- the vendor sets us on a path to Kerberos authentication.

Finally, we acknowledge that we've not built a perfect solution that meets everyone's needs -- the prototype is *an* ID-AUTH service but it would be very presumptuous to call it *the* ID-AUTH service for the campus at large. By numbers alone the Polaris system is far more pervasive and mission critical. In the interim Microsoft has delivered Windows 2000 Active Directory and much of what we have built is now obsolete -- the NT4 Domain Authentication Service should be replaced by an Active Directory supporting Kerberos, SMB and LDAP authentication protocols; the CSO/PH Directory service should be replaced by the Light-Weight Directory Access Protocol (LDAP) services provided with Active Directory. Nevertheless we have something that will serve us well as we move forward to vendor solutions that implement open protocols.

12-June-2000; (ed) Reg Quinton

Recommendations

The prototype we've delivered is but one small step in the continued evolution of an Institutional Directory and that's a project that's been ongoing for many years. "Where to next?" is an important question as things will continue to evolve. Some observations and recommendations follow:

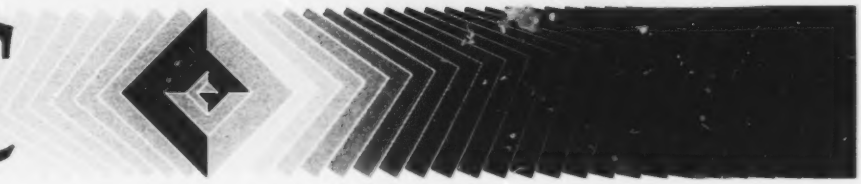
1. We have agreed that the ID-AUTH Project will move towards a *maintenance phase* in the near term, with only minor changes, mostly related to improving the consistency and integrity of the data. During that time, partially as a result of the Active Directory/Windows2000 project, we will gain significant additional knowledge about Active Directory that may prove relevant for the future evolution of UWdir as an Institutional Directory.

2. The ID-AUTH project assumes that the Active Directory/Windows2000 project will articulate some requirements that will be placed on future, production naming in both the Windows2000 and (Internet) DNS contexts. This may result in renaming and/or deprecating the **uwaterloo.ca** authentication service as it now exists (ie. the NT4 Domain name may change). "Authentication service" is intentional, and not the same as the "Identification service" on the diagram.

3. A future phase of the ID-AUTH project should re-examine the implementation and underlying technologies of the "Identification service."

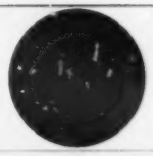
There are many recommendations implicit in other sections of this paper -- see especially the Lessons Learned. The list above is a capsule summary of the larger issues that will shape where we go next.

SPEC



SELECTED RESOURCES

ASSOCIATION OF RESEARCH LIBRARIES



OFFICE OF LEADERSHIP AND MANAGEMENT SERVICES

Books and Journal Articles

American Library Association. "Policy Concerning Confidentiality of Personally Identifiable Information about Library Users." 9 January 2001. <http://www.ala.org/alaorg/oif/pol_user.html>

American Library Association. "Policy on Confidentiality of Library Records." 10 October 2000. <http://www.ala.org/alaorg/oif/pol_conf.html>

Artz, Noam and Daryl Chertcoff. "Web Security Solutions: Central Authentication for Locally Developed Applications." *CAUSE/EFFECT* 22, no. 3 (1999): 50–53. <http://www.educause.edu/ir/library/html/cem993c.html>

Canton, Scott. "The ICAAP Project, Part Three: OSF Distributed Computing Environment." *Library Hi Tech* 15, no. 1–2 (1997): 79–83.

Clark, Elizabeth. "Product Focus: Authentication Devices take on a New Identity." *NetworkMagazine.com* (14 June 2000) <http://www.networkmagazine.com/article/NMG20000612S0009>

Cole, Timothy W. "Using Bluestem for Web User Authentication and Access Control of Library Resources." *Library Hi Tech* 15, no. 1–2 (1997): 58–71.

Cox, Andrew. "Authentication & Authorization: A Guide." 23 May 2000. <http://litc.sbu.ac.uk/candleathens/>
— "Glossary." <http://litc.sbu.ac.uk/candleathens/glossary.html>
— "Solutions." <http://litc.sbu.ac.uk/candleathens/solutions.html#projects>
— "12 Key Readings—on Authentication and Authorization." <http://litc.sbu.ac.uk/candleathens/readings.html#12key>

Digital Library Foundation. "A Digital Library Authentication and Authorization Architecture." 22 March 2000. <http://www.ucop.edu/irc/cdl/tasw/Authentication/Architecture-3_W95.pdf>

EDUCAUSE. "PKI and Security for Higher Education: White Paper." 24 September 1999. <http://www.educause.edu/netatedu/contents/groups/pkiwhtpaper_990923.pdf>

EDUCAUSE. "PKI and Security for Higher Education Workshop." A workshop of the EDUCAUSE Net@EDU Program held at Snowmass Village, Colorado, 12–13 August 1999. <http://www.educause.edu/netatedu/contents/events/aug99/proceedings.html>

Esterhazy, Jonathan. "Providing Authenticated Access to Web Resources." 1 February 1999. <http://www.umanitoba.ca/academic_support/libraries/units/lets/web/cni99/proxy-paper.pdf>

Feghhi, Jalal, Peter Williams, and Jelil Feghhi. *Digital Certificates: Applied Internet Security*. Reading, MA: Addison-Wesley, 1999.

Garfinkel, Simson, Gene Spafford, and Debby Russell. *Web Security, Privacy and Commerce*. 2nd Edition. Cambridge: O'Reilly, 2001.

Gladney, H.M. and Arthur Caniu. "Authorization Management for Digital Libraries." *Communications of the ACM* 44. no. 5 (2001): 63–65.

Glenn, Ariel and David Millman. "Access Management of Web-based Services: An Incremental Approach to Cross-organizational Authentication and Authorization." *D-Lib Magazine* (September 1998). <http://www.dlib.org/dlib/september98/millman/09millman.html>

Goerwitz, Richard. "Pass-Through Proxying as a Solution to the Off-Campus Web-Access Problem." Brown University Scholarly Technology Group. <http://www.stg.brown.edu/pub/proxydoc/report.shtml>
Shorter version in *D-Lib Magazine* (June 1998). <http://www.dlib.org/dlib/june98/stg/06goerwitz.html>

Guillou, Louis C., Michael Ugon, and Jean-Jacques Quisquater. "Cryptographic Authentication Protocols for Smart Cards." *Computer Network* 36 (2001): 437–451.

Harbitter, Alan and Daniel A. Menasce. "Performance of Public-Key-Enabled Kerberos Authentication in Large Networks." *IEEE Symposium on Security and Privacy* (2001): 170–83.

Housley, Russ and Tim Polk. *Planning for PKI: Best Practices Guide for Deploying Public Key Infrastructure*. New York: John Wiley, 2001.

Internet Council of the National Automated Clearing House Association (NACHA). "The Internet Council." <http://internetcouncil.nacha.org/>

Internet Engineering Task Force. Common Authentication Technology (CAT) Working Group. "Common Authentication Technology (cat)." 31 July 2001. <http://www.ietf.cnri.reston.va.us/html.charters/cat-charter.html>

Jenkins, Ruth. "Clashing with Caching?" *Ariadne* 21 (20 September 1999) <http://www.ariadne.ac.uk/issue21/web-cache/>

JSTOR. "[Options for] Remote Authentication." 14 September 2001. <http://www.jstor.org/about/authentication.html>

Kubaitis, Ed. "Bluestem Protocol Walkthrough (1.1.2)." University of Illinois at Urbana-Champaign. August 2000. <http://ejk.cso.uiuc.edu/ejk/bluestem/protocol.html>

Lavagnino, Merri Beth. "The ICAPP Project, Part One: A Continuum of Security Needs for the CIC Virtual

Library." *Library Hi Tech* 15, no. 1–2 (1997): 72–76.

Lynch, Clifford A. "The Changing Role in a Networked Information Environment." *Library Hi Tech* 15, no. 1–2 (1997): 30–38.

—— "A White Paper on Authentication and Access Management Issues in Cross-Organizational Use of Networked Information Resources." Revised discussion draft of April 14, 1998. 6 August 2001. <http://www.cni.org/projects/authentication/authentication-wp.html>

—— "Access Management for Networked Information Resources." *CAUSE/EFFECT* 21, no. 4(1998). <http://www.educause.edu/ir/library/html/cem9842.html>

Massachusetts Institute of Technology. "Kerberos: The Network Authentication Protocol." 9 December 2000. <http://web.mit.edu/kerberos/www/index.html>

Nash, Andrew. *PKI: Implementing & Managing E-Security*. New York: McGraw-Hill Professional, 2001.

Potter, Liz and Mark Bide. "User Authentication and Access Management." *Publishing Research Quarterly* (Summer 1999): 24–29.

Rezmierski, Virginia and Aline Soules. "Security vs. Anonymity: The Debate over User Authentication and Information Access." *EDUCAUSE Review* (March/April 2000): 22–30. <http://www.educause.edu/ir/library/pdf/erm0022.pdf>

Riddle, Bob. "The ICAAP Project, Part Two: The Web Architecture." *Library Hi Tech* 15, no. 1–2 (1997): 77–78, 95.

Ross, Michael and Jeff Rubin. "Authentication Gets Tough." *Network Computing* (28 May 2001). <http://www.networkcomputing.com/1211/1211f2.html>

"Secure Web-based Access to High Performance Computing Resources." *ITL Bulletin* (January 1999). <http://www.itl.nist.gov/lab/bulletns/jan99.htm>

Shim, Wonsik "Jeff," Charles R. McClure, and John Carlo. "Measures and Statistics for Research Library Networked Services: ARL E-Metrics Phase II Report." *ARL: A Bimonthly Report on Research Library Issues and Actions from ARL, CNI, and SPARC* (December 2001): 8–9.

Smith, Richard E. *Authentication: From Passwords to Public Keys*. Boston: Addison-Wesley, 2002.

Squid. "Squid Web Proxy Cache." 10 December 2001. <http://squid.nlanr.net/>

Stein, Lincoln. *Web Security: A Step-By-Step Reference Guide*. Reading, MA: Addison-Wesley, 1998.

Stein, Lincoln and John Stewart. "The World Wide Web Security FAQ." 12 September 2001. <http://www.w3.org/Security/faq/www-security-faq.html>

Thawte Consulting. "Digital C· ıtificate FAQs." 22 November 2001. <http://www.thawte.com/support/crypto/certs.html>

Useful Utilities. "EZproxy." 30 November 2001. <http://www.usefulutilities.com/ezproxy/>

VeriSign. "Introduction to Public Key Cryptography." 1998. <http://www.verisign..om/repository/crptintr.html>

All links verified December 11, 2001.

SPEC KIT ORDER FORM

QTY	TITLE		QTY	TITLE		QTY	TITLE	
			____	SP221	Evol & Status of Approval Plans	____	SP161	Travel Policies
			____	SP220	Internet Training	____	SP160	Preservation Org & Staff
			____	SP219	TL 2: Geographic Info Systems	____	SP159	Admin of Lib Computer Files
			____	SP218	Info Technology Policies	____	SP158	Strategic Plans
			____	SP217	TL 1: Electronic Reserves	____	SP157	Fee-based Services
			____	SP216	Role of Libs in Distance Ed	____	SP156	Automating Authority Control
			____	SP215	Reorg & Restructuring	____	SP155	Visiting Scholars/Access
			____	SP214	Digit Tech for Preservation	____	SP154	Online Biblio Search
			____	SP213	Tech Svcs Workstations	____	SP153	Use of Mgt Statistics
			____	SP212	Non-Librarian Professionals	____	SP152	Brittle Books Program
			____	SP211	Library Systems Office Org	____	SP151	Qualitative Collect Analysis
			____	SP210	Strategic Planning	____	SP150	Bldg Security & Personal Safety
			____	SP209	Library Photocopy Operations	____	SP149	Electronic Mail
			____	SP208	Effective Library Signage	____	SP148	User Surveys
____	SP267	User Authentication	____	SP207	Org of Collection Develop	____	SP147	Serials Control/Deselection
____	SP266	Staffing the Library Website	____	SP206	Faculty Organizations	____	SP146	Lib Dev Fund Raising Capabilit
____	SP265	Instructional Support Services	____	SP205	User Surveys in ARL Libs	____	SP145	Lib Publications Programs
____	SP264	Extended Library Hours	____	SP204	Uses of Doc Delivery Svcs	____	SP144	Building Use Policies
____	SP263	Numeric Data Services	____	SP203	Reference Svc Policies	____	SP143	Search Proced Sr LibAdmin
____	SP262	Preservation & Digitization	____	SP202	E-journals/Issues & Trends	____	SP142	Remote Access Online Cats
____	SP261	Post-Tenure Review	____	SP201	E-journals/Pol & Proced	____	SP141	Approval Plans
____	SP260	Interview Process	____	SP200	2001: A Space Reality	____	SP140	Performance Appraisal
____	SP259	Fee-based Services	____	SP199	Video Collect & Multimedia	____	SP139	Performance Eval: Ref Svcs
____	SP258	Corporate Annual Reports	____	SP198	Automating Preserv Mgt	____	SP138	University Copyright
____	SP257	MLS Hiring Requirement	____	SP197	Benefits/Professional Staff	____	SP137	Preservation Guidelines
____	SP256	Changing Roles of Lib Profs	____	SP196	Quality Improve Programs	____	SP136	Managing Copy Cataloging
____	SP255	Branch Libs/Discrete Collectns	____	SP195	Co-op Strategies in Foreign Acqs	____	SP135	Job Analysis
____	SP254	Managing Printing Services	____	SP194	Librarian Job Descriptions	____	SP134	Planning Mgt Statistics
____	SP253	Networked Info Services	____	SP193	Lib Develop & Fundraising	____	SP133	Opt Disks: Storage & Access
____	SP252	Supprt Staff Classifictn Studies	____	SP192	Unpub Matls/Libs, Fair Use	____	SP132	Library-Scholar Communication
____	SP251	Electronic Reference Service	____	SP191	Prov Pub Svcs Remote User	____	SP131	Coll Dev Organization
____	SP250	TL10: Educating Faculty	____	SP190	Chang Role of Book Repair	____	SP130	Retrospective Conversion
____	SP249	Catalogng of Resrces Digitized	____	SP189	Liaison Svcs in ARL Libs	____	SP129	Organization Charts
____	SP248	Licensing of Electronic Prodcts	____	SP188	Intern, Residency & Fellow	____	SP128	Systems File Organization
____	SP247	Management of Lib Security	____	SP187	ILL Trends/Staff & Organ	____	SP127	Interlibrary Loan
____	SP246	Web Page Devel & Managmnt	____	SP186	Virtual Library	____	SP126	Automated Lib Systems
____	SP245	Electronic Reserves Operations	____	SP185	System Migration	____	SP125	Tech Svcs Cost Studies
____	SP244	TL 9: Renovatn & Reconfigurtn	____	SP184	ILL Trends/Access	____	SP124	Barcoding of Collections
____	SP243	TL 8: Users with Disabilities	____	SP183	Provision of Comp Print Cap	____	SP123	Microcomp Software Policies
____	SP242	Library Storage Facilities	____	SP182	Academic Status for Libns	____	SP122	End-User Search Svcs
____	SP241	Gifts and Exchange Function	____	SP181	Perf Appr of Collect Dev Libn	____	SP121	Bibliographic Instruction
____	SP240	Marketing and PR Activities	____	SP180	Flexible Work Arrangem'ts	____	SP120	Exhibits
____	SP239	Mentoring Programs in ARL	____	SP179	Access Services Org & Mgt	____	SP119	Catalog Maintenance Online
____	SP238	ARL GIS Literacy Project	____	SP178	Insuring Lib Colls & Bldgs	____	SP118	Unionization
____	SP237	Managing Food and Drink	____	SP177	Salary Setting Policies	____	SP117	Gifts & Exchange Function
____	SP236	TL 7: E Theses/Diss	____	SP176	Svcs for Persons w/Disabilities	____	SP116	Organizing for Preservation
____	SP235	Collaborative Coll Managmnt	____	SP175	Scholarly Info Centrs	____	SP115	Photocopy Services
____	SP234	TL 6: Distance Learning	____	SP174	Expert Systems	____	SP114	Binding Operations
____	SP233	ARL in Extension/Outreach	____	SP173	Staff Recognition Awards	____	SP113	Preservation Education
____	SP232	Use of Teams in ARL	____	SP172	Information Desks	____	SP112	Reorg of Tech and Pub Svcs
____	SP231	Cust Service Programs in ARL	____	SP171	Training of Tech Svc Staff	____	SP111	Cooperative Collection Dev
____	SP230	Affirmative Action in ARL	____	SP170	Organization Charts	____	SP110	Local Cataloging Policies
____	SP229	Evaluating Acad Libr Dirs	____	SP169	Mgt of CD-ROM	____	SP109	Staff Training for Automation
____	SP228	TL 5: Preserving Digital Info	____	SP168	Student Employment	____	SP108	Strategic Planning
____	SP227	Org of Doc Coll & Svcs	____	SP167	Minority Recruitment	____	SP107	University Archives
____	SP226	TL 4: After the User Survey	____	SP166	Materials Budgets	____	SP106	Electronic Mail
____	SP225	Partnerships Program	____	SP165	Cultural Diversity	____	SP105	Nonbibliographic Dbases
____	SP224	Staff Training & Development	____	SP164	Remote Storage	____	SP104	Microcomputers
____	SP223	TL 3: Electronic Scholarly Pubn	____	SP163	Affirmative Action	____	SP103	Asst/Assoc Dir Position
____	SP222	Electronic Resource Sharing	____	SP162	Audiovisual Policies	____	SP102	Copyright Policies

QTY	TITLE		QTY	TITLE		QTY	TITLE	
____	SP101	User Studies	____	SP067	Affirm Action Programs	____	SP033	Intergrat Nonprint Media
____	SP100	Collection Security	____	SP066	Planning Preserv of Lib Materials	____	SP032	Prep, Present Lib Budget
____	SP099	Branch Libraries	____	SP065	Retrospective Conversion	____	SP031	Allocation of Resources
____	SP098	Telecommunications	____	SP064	Indirect Cost Rates	____	SP030	Support Staff, Student Assts
____	SP097	Building Renovation	____	SP063	Collective Bargaining	____	SP029	Systems Function
____	SP096	Online Catalogs	____	SP062	Online Biblio Search Svcs	____	SP028	Gifts & Exchange Function
____	SP095	Lib Materials Cost Studies	____	SP061	Status of Librarians	____	SP027	Physical Access
____	SP094	Fund Raising	____	SP060	Lib Materials Cost Studies	____	SP026	Bibliographic Access
____	SP093	User Instructions for Online Cats	____	SP059	Microform Collections	____	SP025	User Statistics and Studies
____	SP092	Interlibrary Loan	____	SP058	Goals & Objectives	____	SP024	User Surveys
____	SP091	Student Assistants	____	SP057	Special Collections	____	SP023	Grievance Policies
____	SP090	Integrated Lib Info Systems	____	SP056	External Communication	____	SP022	Private Foundations
____	SP089	Tech Svcs Cost Studies	____	SP055	Interni Com/Staff & Superv Role	____	SP021	Paraprofessionals
____	SP088	Corporate Use of Research Libs	____	SP054	Internal Com/Policies & Proced	____	SP020	Managerial Technical Specialists
____	SP087	Collect Descript/Assessment	____	SP053	Performance Appraisal	____	SP019	Staff Allocations
____	SP086	Professional Development	____	SP052	Cost Studies & Fiscal Plan	____	SP018	Staff Development
____	SP085	Personnel Classification Sys	____	SP051	Professional Development	____	SP017	Library Instruction
____	SP084	Public Svcs Goals & Objectvs	____	SP050	Fringe Benefits	____	SP016	Reclassification
____	SP083	Approval Plans	____	SP049	Use of Annual Reports	____	SP015	Goals & Objectives
____	SP082	Document Delivery Systems	____	SP048	External Fund Raising	____	SP014	Performance Review
____	SP081	Services to the Disabled	____	SP047	Automated Cataloging	____	SP013	Planning Systems
____	SP080	Specialty Positions	____	SP046	Plan Future of Card Catalog	____	SP012	Acquisition Policies
____	SP079	Internships/Job Exchanges	____	SP045	Changing Role Personnel Officer	____	SP011	Collection Development
____	SP078	Recruitment-Selection	____	SP044	Automated Acquisitions	____	SP010	Leave Policies
____	SP077	Use of Small Computers	____	SP043	Automated Circulation Sys	____	SP009	Tenure Policies
____	SP076	Online Biblio Search Svcs	____	SP042	Resource Sharing	____	SP008	Collective Bargaining
____	SP075	Staff Development	____	SP041	Collection Assessment	____	SP007	Personnel Class Schemes
____	SP074	Fees for Services	____	SP040	Skills Training	____	SP006	Friends of the Lib Organization
____	SP073	External User Services	____	SP039	Remote Storage	____	SP005	Performance Review
____	SP072	Executive Review	____	SP038	Collection Dev Policies	____	SP004	Affirmative Action
____	SP071	User Surveys: Eval of Lib Svcs	____	SP037	Theft Detection & Prevent	____	SP003	A Personnel Organization
____	SP070	Preservation Procedure	____	SP036	Allocation Materials Funds	____	SP003	Status of Librarians
____	SP069	Prep Emergencies/Disasters	____	SP035	Preservation of Lib Materials	____	SP002	Personnel Survey (flyer only)
____	SP068	AACR2 Implement Studies	____	SP034	Determin Indirect Cost Rate	____	SP001	Organization Charts

SPEC Price Information (ISSN 0160 3582)

- ❑ Subscription (6 issues per year; shipping included): $190 ARL members/$260 U.S. and Canada nonmembers/$330 international customers.
- ❑ Individual Kits: $35 ARL members/$45 nonmembers, plus shipping and handling.
- ❑ Individual issues of the Transforming Libraries (TL) subseries: $28, plus shipping and handling.

Payment Information

Make check or money order payable in U.S. funds to the **Association of Research Libraries**, Federal ID #52-0784198-N.

Purchase Order # _____

Credit Card: ____ MasterCard ____ Visa Exp date _____

Account # _____

Account holder _____

Signature _____

Ship To

Name _____

Institution _____

Address (UPS will not deliver to P.O. boxes)

_____

_____

_____

Phone _____

Fax _____

Email _____

Shipping & Handling

U.S.: UPS Ground delivery, $6 per publication.

Canada: UPS Ground delivery, $15 per publication

International and rush orders: Call or email for quote.

Total Shipping $_____ **Total Price** $_____

163

Send orders to: ARL Publications Distribution Center, PO Box 531, Annapolis Junction, MD 20701-0531
phone (301) 362-8196 fax (301) 206-9789, email pubs@arl.org

Order online at: http://www.arl.org/pubscat/index.html

U.S. Department of Education
Office of Educatonal Research and Improvement (OERI)
National Library of Education (NLE).
Educational Resources Information Center (ERIC)

REPRODUCTION RELEASE
(Specific Document)

NOTICE

REPRODUCTION BASIS

☒ This document is covered by a signed "Reproduction Release (Blanket) form (on file within the ERIC system), encompassing all or classes of documents from its source organization and, therefore, does not require a "Specific Document" Release form.

☐ This document is Federally-funded, or carries its own permission to reproduce, or is otherwise in the public domain and, therefore, may be reproduced by ERIC without a signed Reproduction Release form (either "Specific Document" or "Blanket").